Attribute Based Data Sharing in Cloud for Cardiac System

Heena Akbar Mujawar¹, Zakir Mujeeb Shaikh²
Department of Computer Science and Engineering
NK Orchid College of Engineering & Technology Solapur, Maharashtra, India

Abstract:
The researchers make available information on basis of race, religion, age, gender, medical history which can be easily available to third party. If sharing of data is made available privacy becomes concern as all data of patient is made visible. Health Data has another face with shortage of facilities. As in India about 70% of population residing in towns and villages lacks facility of angiography and angioplasty in nearby hospital to acquire such facility patient need to travel instead they have ECG facility the patient has to travel approximately 100 KM in some cases more than 100 KM to get these two facilities which is inconvenient in emergency case. Our proposed system helps in sharing of data on public cloud based on the attributes. Attributes are used for retrieving patient data therefore as per needed information will be retrieved and all other data will remain hidden.

Keywords: Cloud, HL7, EMR, Attribute, IaaS, Encryption

I. INTRODUCTION

It is important to consider in medical health record, which has the information and why it was created and how we can provide security. In addition, individuals researchers require health data to improve the medicine or other concern. Health systems create medical records generally refer as Electronic Medical Record, when they treat patients. Records may include medical history, individual's lifestyle and family background, age, vegetarian or non-vegetarian. They may also include laboratory test results, prescription, surgery results, genetic testing results, and research participation. Health and medical information is also collected from individuals when they apply for disability, life or accident insurance through private insurers or government programs. In addition, individuals often generate health and medical related information themselves. They search for illnesses and medical products online, they join support groups, they use mobile applications to monitor their health and fitness, and the list goes on. All the data about health is not secured as people are very much concern for such information. Among different diseases cardiac diseases are lagging of security as patient complete data can be leaked easily. The diagnosis is issue for cardiac related diseases as people living in small villages lack facilities related to angioplasty and angiography. If there’s emergency patient has to rush for multi specialist hospital and patient has to travel approximately 100 KM some time more than 100KM. Another issue is as researcher get information for diagnosis through religion, age, gender and medical history and check patient’s life style if individual prefers veg or non-veg in his daily eating. The cloud computing have a great impact on network security which has various service models (public, private, hybrid). The public cloud is a standard service model which is used basically for storage purpose. Our system will make use of public cloud which will encrypt data and store in patient database and with symmetric key the encrypted data is Decrypted and data is retrieved on attribute based which will be given to user as well as stored on cloud.

Figure. 1. Public Cloud

II. RELATED WORK

A. Previous work

The existing system Personnel health record (PHR) is considered as a standard for storing health records. The PHR system also reduce paper work in maintaining health records, helps in minimizing time and reduces the cost of storage. The system provides interoperability between Personnel health record and Electronic Health records (EHR). The features is provides Appointment scheduling, medication renewals, pre-appointment questionnaires, and sharing of complete test results in two ways. The first way modeled the data supporting these functions being provided electronically but still requiring manual processing. For example, a PHR appointment scheduling function sending a secure message to a provider’s office that then still needed to be manually entered into the provider’s appointment scheduling system. The second way envisioned data from PHR functions that allowed for automatic processing of the data from the PHR to the EHR, analogous to how several on-line services allow for direct scheduling of airline flights. Although the initial costs of building to a data standard structure are roughly the same as building to a unique, nonstandard data structure, the benefits of a totally standardized and automated PHR function are significantly greater than one that still requires some degree of manual processing because of a unique, non-standard data structure. The analysis helps identify costs and benefits to providers who currently bear direct healthcare costs. The existing system has disadvantage patients, employers and non-healthcare related corporations may derive significant benefits from PHRs. The system improved convenience, quality of care, safety, communication, record
keeping, and efficiency through the use of PHRs. However, the evidence for hard cost savings and value by these other groups, including patients, has not been demonstrated, and was not included in our model.

III. PRELIMINARIES

A. Abbreviations and Acronyms

HL7: Health Level Seven is a standard for exchanging information between medical applications. This standard defines a format for the transmission of health-related information. Examples of HL7 messages include patient records, laboratory records and billing information.

ASCII: American Standard Code for Information Interchange. ASCII is a standard that assigns letters, numbers, and other characters within the 256 slots available in the 8-bit code.

AES: Advanced Encryption standard i.e. Rijndael (pronounced rain-dahl) is the algorithm that has been selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES). It was selected from a list of five finalists that were themselves selected from an original list of more than 15 submissions. Rijndael will begin to supplant the Data Encryption Standard (DES)

IV. SYSTEM AND THREAT MODELS

A. System Models

The public cloud deployment model represents true cloud hosting. In this deployment model, services and infrastructure are provided to various clients. This model is best suited for business requirements wherein it is required to manage load spikes, host SaaS applications, utilize interim infrastructure for keeping patient data, and manage their research material which are consumed by many users that would otherwise require large investment in infrastructure from businesses. Our system works on public cloud. Our system provides entities which are depicted in figure 1. The cloud which stores data where the plaintext in converted in to HL7 and using Rain ideal the patient data encrypted and is stored on cloud the Figure 2 the brief process of data to save on cloud. In Figure 3 the detail process of managing different key to each attribute are shown in database model. The client has to perform registration and they are provided with key during decryption data according to attribute is retrieved.

B. Security Requirements

In this paper, we made effort to meet the following main security requirements for data sharing in cloud with attribute base for cardiac data:

1) Privacy: The cardiac data of patient should be miss used by third party.

2) Scalable: The shared data should be made easily available in emergency case.

3) Hiding of data: The data is retrieval on attribute base and all other data is invisible

V. CONCLUSION

In this paper the patient cardiac data in converting to HL7 and applying encryption technique i.e. Advanced Encryption Standard (Rijndael Encryption). Once the data is stored in Cloud the researchers and other registered users or clients can access the data for their research purpose. While allowing researchers to access the data is based on the attribute or the patient data. Only that attribute will decrypted and other will remain in encrypted format. Using this technique we preserving the patient data as well as helping the researchers to carry out their research. In other usage if the patient forgot their file to carry then the patient or relative of patient can share the key to respective doctors. Hence the system helps a lot to research, self and other hospitals

VI. REFERENCES


[6] Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability Yue Tong, Student Member, IEEE, Jinyuan Sun, Member, IEEE, Sherman S. M. Chow, and Pan Li, Member, IEEE