International Journal of Trend in Research and Development, Volume 3(3), ISSN: 2394-9333
www.ijtrd.com

Towards Auditable and Secure Access to Health Data in Public Cloud

[1]C M Parameshwarappa, [2]Akkamahadevi C, [3]Dr Naghabushana and [4]Dr Aravinda T V
[1]Head of Department, [2]M.Tech Student, [3]Professor and HOD, [4]Professor,
[1,2,3,4]Department of CSE, Sri Taralabalu Jagadguru Institute of Technology, Ranebennur, India

Abstract: Inspired by the privacy issues, curbing the adoption of electronic healthcare systems and the huge success of cloud service models, we propose to incorporate privacy into e-health care systems with the help of private cloud. Our system offers remarkable components including privacy preserving data storage, retrieval, and monitoring and auditability of users. Proposed system also incorporate the idea of symmetric and asymmetric encryption and decryption techniques with limit marking for giving part based access control based on the role of the users whether he/she is a doctor or patient in both normal and emergency cases. Anytime anywhere accessibly electronic health care system works assume a crucial part in our everyday life. Administrators upheld by cell phones, for example, home care and remote observing, empower patients to hold their living style and reason negligible interference to their every day exercises. Furthermore, it altogether decreases the hospital occupancy, permitting patients with higher need of in-doctor's facility treatment to be admitted.

Keywords: *Private Cloud, Privacy, auditability, Encryption, e-Health, Hospital Occupancy.*

I. INTRODUCTION

Quick access to health related information is very important. With quick access to health related facts good health services can be specified, by keeping track on health we can improve our life style by which quality of life is transformed, Anywhere at whatever time it is open electronic social health organism assume an imperative part in our daily life. There are various services regarding the health through mobiles, homecare services and distant monitoring are some of the examples of mobile services by making use of these patients can follow a clean life style with less disorders. Along with these it reduces the patient's energy of visiting the hospital again and again, only the patients with complex need can be admitted to the hospital for better handling.

With e-health services structures are becoming progressively widespread, these service structures includes a lot of individual information for therapeutic reason. There is a great need for keeping health information privately and constraining the entrance. For example a trade person may opt not to deal someday with explicit illness[1]. Another example where in insurance agency may decline to give life coverage for the person knowing the health history of patients.

Even though lots of services provided by a e-health service, at technical level privacy issues are not addressed sufficiently and efforts are being made in order to keep health data secure but they are quite fallen short. Since maintaining in the confidentiality in the cyberspace is significantly more difficult and challenging. Thus e-health systems need to be developed with promising privacy and security to protect patient's information.

Cloud computing is a wide spread area where in storing the data, retrieving the data and carrying out the computation using the data is very popular. Private cloud is being introduces which provide service to the mobile users. The suggested cloud assisted system administration is enlivened by the force, comfort and cost effectiveness of the cloud based information outsourcing worldwide.

II. RELATED WORK

Some early works on privacy protection for e-health data concentrate on the framework design [2], including the demonstration of the significance of privacy for e-health systems, the authentication based on existing wireless infrastructure, the role-based approach for access restrictions, etc.

In particular, a practical Identity Based Encryption scheme in the random oracle model was proposed by Boneh and Franklin [5]. It has been used [3] for the purpose of enforcing simple role-based cryptographic access control. Using identity value, any person can generate the public key in identity-based systems even without distributing the key between the individuals messages can be encrypted.

Among the earliest efforts on e-health privacy, medical Information Privacy Assurance (MIPA) [4] pointed out the importance and unique challenges of medical information privacy, and the devastating privacy breach facts that resulted from insufficient supporting technology. There is a need for the privacy of the medical data. Mentioning the privacy of the medical data is not so easy it is a great challenge. Mentioning the privacy of the medical data, challenges that need to be faced in order to maintain the privacy is being pointed out in the MIPA. In MIPA a unique technology is being introduced by which privacy can easily established. The special feature in this is that individuals protect their own data. Individual encrypt relevant information and place on the server.

Privacy preserving health data storage is studied by Sun et al.[6], where patients encrypt their own health data and store it on a third party server. This works on Searchable Symmetric encryption (SSE). In this, encrypted data by the individuals need to be stored on the remote server and the same data which is being stored need to be retrieved when necessary. While retrieving data, there is need to be properly searched among huge data content. All this activity of storing, searching and retrieving is being carried out by the searchable symmetric encryption.

The proposed concept of Patient-controlled encryption(PCE) was proposed by Benaloh et al [7]. In this, the health data may be decayed into number of hierarchy of tiny piece of information which can be encrypted using the key that are under the control of patients. Here providing Symmetric key

PCE for flexible hierarchy from RSA and providing symmetric key PCE and public key PCE for fixed hierarchy.

An attribute-based encryption (ABE) [8] can be proposed by Chase and Chow for fine-grained access control. This encryption allows break-glass access via the use of emergency attributes. This type of encryption is mainly being carried out for sensitive data. Providers or owner using a set of attributes will encrypt the data .If any other person want to access the data then there are being provided with the access structure by the owner. If access structure matches the attribute then decrypted data will be obtained.

A personal and pervasive (PPcare) health care system for the elders was proposed by Zenyuchn and Yqiang[9], shows how the elderly health data can be monitored and kept track using PP care. PP care is system mainly for elderly persons. System is mobile based; using mobile monitoring of the health is carried out. Sport scheduling, calories intake, Rapid change alert and physiological tables nursing are the four major functionalities that the system include.

The secured health m-healthcare system was proposed by Ganeshan and Hrish[10], about EMR. EMR is nothing but Electronic Medical Records. This system provides various facilities to the use by which data tracking can be carried at various times, patients can be provided with the description online itself, monitoring of the patients would be easy using this system. Only the valid user can access the system. Security is provided to the data by encrypting the data and when data need to be reviewed back it will be decrypted.

A. Existing System Disadvantages

In order to maintain the health data privacy, to have health care during emergency condition HCPP system is used. In HCPP system search and access method will not be hidden.

Elderly health data is monitored and kept track using PP care. PP care is system mainly for elderly persons. System is mobile based; using mobile monitoring of the health is carried out. Sport scheduling, calories intake, Rapid change alert and physiological tables nursing are the four major functionalities that the system include.

Electronic healthcare system (e-health care systems) are increasingly popular, a large amount of personal data for medical purpose are involved, and people start to realize that they would completely loss control over their personal information once it enters into the cyberspace. According to the government website, around 8 million patients health information was leaked in the past two years. There are good reasons for keeping medical health data private and limiting the access. An employer may decide not to hire someone with certain diseases. An insurance company may refuse to provide life insurance knowing the disease history of a patient.

Disadvantages

- Privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short.
- The storage privacy in the existing system is weaker form of privacy because it does not hide search and access patterns.
- There is a shortage of viable protocols, architectures, and systems assuring privacy and security to safeguard sensitive and personal digital information.

III. PROPOSED SCHEME

The proposed system provided here is an e-health services system which is built on soft as a service model as shown in fig1.This SaaS provide the service of the private cloud by making use of the infrastructure of the public cloud. The users will provide there information to the private cloud this in turn store the data on public cloud. The proposed service provides privacy by carrying out intensive calculation on cloud sendoff simple tasks to users.

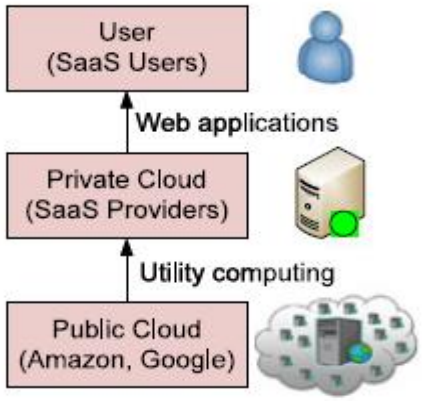

Figure 1: SaaS model

Privacy and security are key features essential for every system. In health care system proposed here privacy is achieved by making use of private cloud. Adoptive key management, Information storage and recovery during emergency conditions by mentioning privacy, through assessment to avoid misuse of data, are important features of healthcare system proposed here. In order to maintain privacy in the system safe indexing mechanism, which hides pattern for searching and accessing key word, is used. In order to generate random numbers, key managements are:

"Software as a Service" SaaS: e-health application need to run on the infrastructure of cloud. SaaS is one of the applications, even a layer that provide the people to run their application. Consider for example, with a thin client interface such as Web browser the applications will be available from several client devices. There is no need for consumer to manage or regulator the core cloud structure such as network, servers, operating systems, storage. The safety and privacy guard is provided as an inbuilt part of the SaaS to the healthcare users when used this type of model.

"Private cloud":Healthcare provision organization especially uses this kind of cloud infrastructure. This shall accomplish either by society or any other person and may exist going on or bad in foundation. There is no need for consumer to manage or regulator the core cloud structure such as network, servers, operating systems, storage. The safety and privacy guard is provided as an inbuilt part of the SaaS to the healthcare users when used this type of model.

"Public cloud": Cloud will be having owner who is known as cloud service provider, the cloud infrastructure is made available to the general users or even a large industry individual when paid. Protecting patients' security and privacy is a great responsibility, the application developers and consumers will be handling its responsibility. The consumer can implement their application on the cloud infrastructure using the tools and the languages which are being provided by cloud.

IV. SYSTEM MODEL

The most important components involved in our system are depicted in fig2.

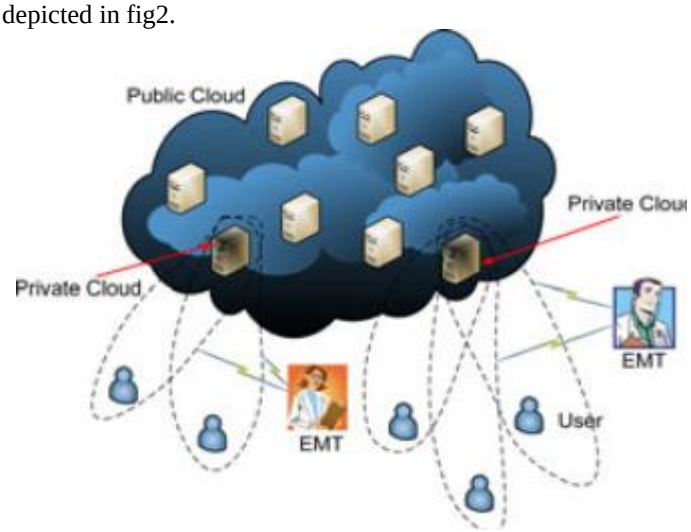

Figure 2: Mobile Health Network with Hybrid Cloud

USER: User collects their health data through by monitoring some devices worn or carried, for ex: Electrocardiogram sensors and health tracking patches.

EMT: Emergency medical technician(EMT) is aa physician who performs an emergency treatment. By user and EMT, we refer the person and the associated computing facilities. The computing facilities are mainly mobile devices carried around such as Smartphone, tablet, or personal digital assistant.

PRIVATE CLOUD: Each user is associated with one private cloud. Multiple private clouds are supported on the same physical server. Private clouds are always online and available to handle health data on behalf of the users. The private cloud will process the data to add security protection before it is stored on the public cloud.

PUBLIC CLOUD: Public cloud is the cloud infrastructure owned by the cloud providers such as Amazon and Google which offers massive storage and rich computational resource.

We assume that at the bootstrap phase, there is a secure channel between the user and he, his/her private cloud. Ex: secure home Wi-Fi network, to negotiate a long term shared key. After the bootstrap phase, the user will send health data over insecure network to the private cloud residing via the internet backbone. But here we do not focus on the location privacy of mobile users which can be leaked when sending health data to the private cloud.

V. SECURITY REQUIREMENTS

The most important security requirements for practical privacy-preserving mobile health care system are as follows:

Auditability: In emergency data access, the users may be physically unable to grant data access or without the perfect knowledge to decide if the data requester is a legitimate EMT. We require authorization to be fine-grained and authorized parties' access activities to leave cryptographic evidence.

Anonymity: In case of emergencies, no particular user can be associated with the storage and retrieval process, i.e., these processes should be anonymous.

Data confidentiality: An unauthorized party for ex: public cloud and outside attackers should not learn the content of the stored data.

Unlink ability: An unauthorized party should not be able to link multiple data files to profile a user. It indicates that the file identifiers should appear random and leak no useful information.

Keyword privacy: The keyword used for search should remain confidential because it may contain sensitive information, which will prevent the public cloud from searching for the desired data files.

Search pattern privacy: During searching of any document with keywords, knowing whether the searches were for the same keyword or not, and the access pattern, i.e., the set of documents that contain a keyword, should not be revealed. This requirement is most challenging and none of the existing efficient SSE can satisfy it. It represents stronger privacy which is particularly needed for highly sensitive applications like health data networks.

CONCLUSION

Incorporate protection in mobile health care system with the assistance of the private cloud, there is a solution for security saving information by utilizing symmetric key encryption and utilizing arbitrary string as key to store and recover health information to and from public cloud. Here there also need to be given solution to which provides access for health data stored on the cloud in both normal and emergency cases. Proposed system provides audit ability of the user to prevent unauthorized access of health data. It also investigates access control and auditability of the authorized people. As few systems have encountered misbehavior, there is chance of loss of data. In order to avoid these kinds of problems we use private cloud for secure access of Health Data in Public cloud which is robust, secure and manages time efficiently together with encryption based on role based approach.

. The future enhancement is to plan to devise mechanisms that can detect whether user's health data have been illegally distributed, and identify possible source(s) of leakage (i.e., the authorized party that did it).

References

[1] U.S. Department of Health & Human Service, "Breaches Affecting 500 or More Individuals," (2001).

[2] P. Ray and J.Wimalasiri, "The need for technical solutions for maintaining the privacy of EHR," in Proc. IEEE 28th Annu. Int. Conf., New York City, NY, USA, Sep. 2006.

[3] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care," presented at the

14th Int. Workshop Database Expert Syst. Appl. Prague, Czech Republic, 2003.

[4] L. Zhang, G. J. Ahn, and B. T. Chu, "A role-based delegation framework for healthcare information systems," in 7th ACM Symp. Access Control Models Technol., Monterey, CA, USA, 2002.

[5] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing. Extended abstract in CRYPTO 2001" SIAMJ Computing.

[6] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronic medical records," in Proc. ACM Workshop Cloud Computing Security, 2009.

[7] U.S. Department of Health & Human Service, "Attribute Based Encryption: Mechanism for Scalable and safe sharing of individual health data in cloud". Zhng, K. Reen, and W. Lu Int. Conf., New York City, NY, USA, Sep. 2006, pp. 486–489.

[8] S.Yu.C.Wang, K.Ren, and W.Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," presented at the IEEE Conf. Comput. Commun., San Diego, CA, USA, Mar. 2010.

[9] U.K.Department of Health & Human Service, "Design and development of secured m-healthcare system". Ganeshan, Hrish. Appl, Prague, Czech Republic, 2004.

[10] J.Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 373–382.

[11] P. Ray and J.Wimalasiri,"PP Care: A personal and pervasive health care system for the elderly". AUTHORS: Taang, Zenyu Chn, Yqiang. Appl, Prague, Czech Republic, 2003.

[12] W. B.Lee and C. D.Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 1, pp. 34–41, Jan. 2008.

[13] Ian Foster, Carl Kesselman, Gene Tsudik and Steven Tuecke, "A Security Architecture for Computational Grids," proc. 5th ACM conference on Computer and communications security, pp. 83–92, 1998.