# A Review on Secured Techniques for Privacy Preserving and Auditability in Cloud-assisted Mobile-access of Health Data

**Radhika Chavan, Prof. S.Y.Raut**

*Abstract*— **Electronic Healthcare System plays a vital role in our daily life. Since valuable and sensitive data of patient need to be shared on cloud environment. Privacy is the foremost concern of patients. This paper propose to give privacy including private cloud and auditability. It also discussed the privacy-preserving data storage, key management, search and access pattern hiding scheme. This paper presented the concept of attribute based encryption with threshold signature to prevent the misbehavior in emergency and normal situation. Attribute based encryption used to provide security and access control.**

*Index Terms*—**Access control, Attribute Based Encryption, Auditability, E-Healthcare, Privacy.**

## I. Introduction

The wave of adopting information and communication technologies in virtually all aspects of life hit the healthcare industry in the early '90s, which has gradually gained momentum ever since as we see most of the modern-day clinical systems partially or fully automated. The digitalization of clinical systems has no doubt increased efficiency and quality of service, and reduced cost, but it has also introduced various security and privacy concerns. The Electronic Health Record (EHR) is the keystone of a medical information system [2]. A survey on clinical information privacy, conducted before the proliferation of the Internet, showed that 80% of the respondents were worried about medical privacy. The mobile Healthcare (m-Healthcare) system has been envisioned as an important application of pervasive computing to improve health care quality and save lives. Specifically, in an m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments [new]. Instead, after being equipped with smart phone and wireless body sensor network (BSN) formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere[12] . Cloud computing is a coalesce of many computing fields and has gained much popularity in the recent years. Cloud computing provides computing, storage, services, and applications over the Internet. Moreover, cloud computing facilitates to reduce capital cost, decouple services from the underlying technology, and provides flexibility in terms of resource provisioning. Although cloud is useful for computing and storage the traditional computation offloading techniques cannot be used for the smartphones directly, because these techniques are generally energy-unaware and bandwidth hungry.

The proposed cloud assisted mobile health networking is inspired by the power, flexibility, convenience and cost efficiency of the cloud-based data outsourcing paradigm [9]. We introduce the private cloud which can be considered as a service offered to mobile users. The proposed solutions are built on the service model shown in Fig. 1. A software as a service (SaaS) provider provides private cloud services by using the infrastructure of the public cloud providers (e.g., Amazon, Google). Mobile users outsource data processing tasks to the private cloud which stores the processed results on the public cloud. The cloud assisted service model supports the implementation of practical privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving mobile users with lightweight tasks [9].

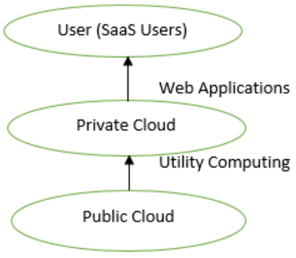

Fig 1 : SaaS Service Model

Software-as-a-Service (SaaS) enables a software deployment model in which one or more applications and the computing resources to run them are provided for use on demand as a turnkey service. It can reduce the total cost of hardware and software development, maintenance, and operations[13].

## II. LITERATURE SURVEY

"A Flexible Role-based Secure Messaging Service: Exploiting IBE Technology for Privacy in Health Care",[3] presented an innovative technical solution in the area of

***Radhika Chavan,*** *Computer Engineering, Pravara Rural Engineering College,Pune University,,Ahmednagar,India,9975662185.*

***Prof.S.Y.Raut****, Computer Engineering, Pravara Rural Engineering College Pune University, Ahmednagar, India, 9689963062.*

secure messaging that exploits Identifier based Encryption (IBE) technology. A secure messaging system based on IBE has been fully implemented and it is currently used in a trial with a UK health service organization. Although that approach is more flexible and simpler than an equivalent approach based on traditional cryptography and PKI technology. A few issues still need to be explored in a broader context, especially regarding the authentication of users with trust authorities.

“Privacy And Emergency Response in E-Healthcare Leveraging Wireless Body Sensor Networks”, [6] provide the details on privacy and security issues in e-healthcare systems and techniques. This paper describes the wireless body sensor network which is very efficient and secure solution to addressed the security and privacy issues. This paper is intended to provide a starting point for developing secure and feasible e-healthcare systems.

“The Need for Technical Solutions for Maintaining the Privacy of EHR”, [2] Pradeep Ray, and Jaminda Wimalasiri presented EHR privacy requirements in the e-health frameworks.

“An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks”, [5] proposed VANET security system mainly achieving privacy and traceability to avoid misbehavior. The technique used here is ID-based cryptosystem. The future work will consists of simulating the proposed security system and experimenting it in real VANET settings.

“HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare” [7] this paper proposed 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.

“PAAS: A Privacy-Preserving Attribute-based Authentication System for eHealth Networks”, [8] proposed a framework of privacy-preserving attribute-based authentication system in eHealth networks. The attribute-based authentication schemes designed for higher privacy levels preserve the more privacy on attributes and attribute values, but cost more computation and communication resources.

In this paper we propose to build privacy into mobile health system.

## III. E-HEALTHCARE SYSTEM DESIGN

Recently, the expeditious development of wireless networks has led to the emergency of a new type of e-healthcare system, providing expert-based medical treatment remotely on time. With the e-healthcare system, wearable sensors and portable wireless devices can automatically monitor individuals' health status and forward them to the hospitals, doctors and related people. The system offers great conveniences to both patients and health care providers For the patients, the foremost advantage is to reduce the waiting time of diagnosis and medical treatment, since they can deliver the emergent accident information to their doctors even if they are far away from the hospital or they don't notice their health condition.

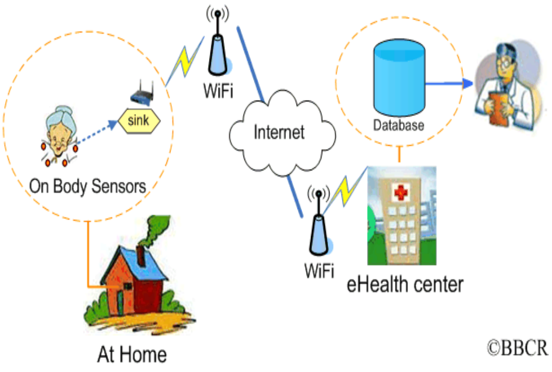

Fig 2: E-Healthcare System

. In addition, e-health system causes little interruption to patients' daily activities. For the health care providers, after receiving the abnormal signals from the patients, appropriate treatment can be made, which saves medical resources [11]. However, to ensure the security and privacy of patients' medical records encounters a lot of challenges: how to achieve the confidentiality and integrity of patients' information, the security of wireless body area network, the privacy and unlink ability of patients' health status, the mutual authentication between patients and hospitals, etc.

## IV. PROPOSED SYSTEM ARCHITECTURE

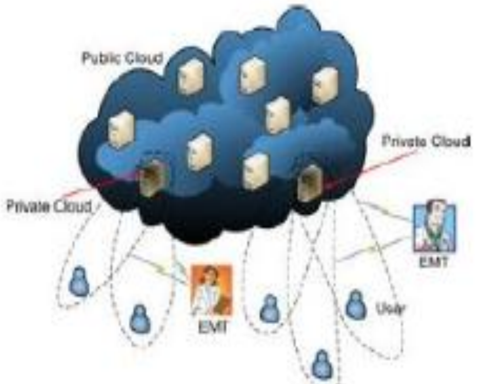

Fig 3: Cloud-assisted mobile health network

Here users collect their health data through the monitoring devices worn or carried, e.g., electrocardiogram sensors and health tracking patches. Emergency medical technician (EMT) is a physician who performs emergency treatment. EMT can access patient’s data only at emergency. 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. This can be very desirable in situations like medical emergencies. The private cloud will process the data to add security protection before it is stored on the 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 his/her private cloud, eg. 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. Note that, we do not focus on the location privacy of mobile users which can be leaked when sending health data to the private cloud [9].

## V. MODULES AND ANALYSIS

### 1] Attribute-Based Encryption

The main goal of Attribute-Based Encryption is to provide security and access control. It is public key based one to many encryption that allows users to encrypt and decrypt data based on user attributes. Attribute-Based Encryption ABE has shown its promising future in fine-grained access control for outsourcing reliable data. Typically, data are encrypted by its sole owner under a set of attributes. Anyone who accesses the data are assigned access structures by the owner and decryption is done only if the structures are matched.

### 2] Threshold Secret Sharing

Basically secret sharing is a cryptographic technique which allows confidential data to be spilt among several storage providers. Threshold Secret Sharing in MIPA is a mechanism for sharing secret information among multiple entities so that the cryptographic power is distributed at the same time to avoid single point of failure. The private cloud will process the data to add security features before it is stored on the cloud domain. Public cloud is owned by the cloud providers such as Amazon and Google which offers massive storage and rich computational resource. The bootstrap phase, there is a secure channel between the user and the private cloud.

### 3] Threshold signature with ABE

Fine-grained access control is achieved by ABE based threshold signing scheme, where the expensive ABE operations are only used for encrypting small secret values and the majority of data encryption is fulfilled by efficient symmetric key scheme. The threshold signature exchange used enables the private cloud to record evidence that is signed by the authorized parties which can be used as audit logs. By having the private cloud and EMT both signing the EMT's data access requests, users can later check whether the request is legitimate and accurate, and obviously be assured that the EMT cannot deny a request and the private cloud cannot falsely accuse an EMT[4].

### 4] Security Fulfillments

The proposed approach guarantees the five storage privacy requirements. First, since the data are encrypted, unauthorized parties cannot learn the content of the stored data. Second, our file indicators are countable values that do not specify any information about the file content or the ownership. So, multiple data files cannot be linked by their identifiers. Third, by adding redundancy to the linked lists, the unknown can rarely say if the searches were for the identical keyword, or if a set of data files contain a same keyword [4]. The fourth requirement, i.e., the storage/retrieval anonymity can be easily satisfied because the private cloud performs the storage/retrieval for all the users it supports and no particular user can be associated with any storage retrieval techniques. Finally, the keyword for the search is encrypted in the trapdoor, and thus, no sensitive information is exposed.

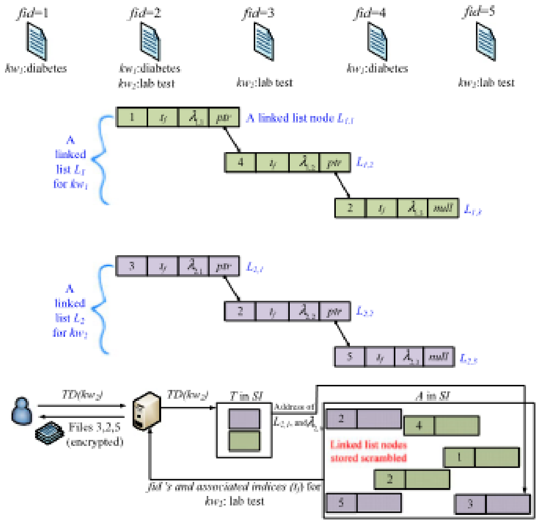

Fig 4: Construction of patient's record with the security fulfillments

## CONCLUSION

Cloud computing, the sensitive data shared among various servers which gives rise to security concerns. This paper proposed work builds privacy into the mobile health systems with the help of the private cloud. Bootstrapping is the secure channel that is used for the private communication of cloud users who have been authenticated and authorized. A solution for privacy-preserving data storage is achieved by integrating a PRF based key management for unlink ability, a search and access pattern hiding scheme based on redundancy, and a secure indexing method for privacy-preserving keyword search. The investigated techniques provide access control (in both normal and emergency cases) and auditability of the authorized parties to prevent misbehavior, by combining ABE-controlled threshold signing with role-based encryption. Future work will plan to devise mechanisms that can detect whether users' health data have been illegally distributed and identify possible sources of leakage.

## REFERENCES

[1] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” *Future Generation Computer Systems*, Vol. 28, No. 3, 2012, pp. 583-592.

[2] P.Ray and J.Wimalasiri,“The need for technical solutions for maintaining the privacy of EHR,” in Proc. *IEEE 28th Annu. Int. Conf.*, NewYorkCity, NY, USA, Sep. 2006, pp. 4686–4689.

[3] M. C. Mont, P. Bramhall, and K. Harrison, “A flexible role-based secure messaging service: Exploiting IBE technology for privacy in healthcare,” presented at the 14th Int. Workshop Database Expert Syst. Appl., Prague, Czech Republic, 2003.

[4] S.Sundar Rajan, P.Nikitha,”Privacy Preserved and Auditable Health Data Access in Cloud using Threshold Signature with ABE based Access Control ,” International Journal of Advanced Research in Science, Engineering and Technology Vol. 2, Issue 2, February 2015

[5] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, “An identity-based security system for user privacy in vehicular ad hoc networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010.

[6] J. Sun, X. Zhu, and Y. Fang, “Privacy and emergency response in e-healthcare leveraging wireless body sensor networks,” *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 66–73, Feb. 2010.

[7]J.Sun,X. Zhu, and Y. Fang,“HCPP:Cryptography based secure HER system for patient privacy and emergency healthcare,” in Proc. *IEEE Int. Conf. Distrib. Comput. Syst.*, Jun. 2011, pp. 373–382.

[8] L. Guo, C. Zhang, J. Sun, and Y. Fang, “PAAS: Privacy-preserving attribute-based authentication system for eHealth networks,” in Proc. *IEEE Intl. Conf. Distrib. Comput. Syst*., Jun. 2012, pp. 224–233.

[9] Yue Tong, Jinyuan Sun, Sherman S. M. Chow, and Pan Li, “Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability” , *IEEE Journal Of Biomedical And Health Informatics*, VOL. 18, NO. 2, MARCH 2014.

[10] Gowresh N, Brundha Elci J, Dr. K.N. Narasimha Murthy,” A Survey on Privacy Preserved Mobile-Access Health Care Data with Auditability using Cloud ”,International Journal of Innovative Research in Computer and Communication Engineering An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 5, May 2015.

[11] Mrinmoy Barua, Rongxing Lu, and Xiaohui Liang ,”Bibliography on Secure E-Healthcare Systems “,Broadband Communications Research (BBCR) Group ,Department of Electrical and Computer Engineering ,University of Waterloo, Waterloo, Ontario, Canada

[12] M.AyishaBeevi1, Dr.G.J Joyce Mary,” Newly secured privacy preserving and Auditability techniques for Cloud Assisted Mobile Access of Health Data ”, SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – volume 2 Issue 3 March 2015.

[13] Wayne A. Jansen, NIST,” Cloud Hooks: Security and Privacy Issues in Cloud Computing ”,Proceedings of the 44th Hawaii International Conference on System Sciences - 2011 .

[14] John Harauz, Lori M. Kaufman, Bruce Potter, “Data Security in the World of Cloud Computing”,Copublished By The IEEE Computer And Reliability Societies. July/August 2009

**Radhika Chavan** received B.E.(I.T.) degree from Shivaji University,M.E. Computer Engineering Student.

**Prof. S.Y.Raut** received M.E. degree and Assistant Professor at PREC,Loni.