Cloud based E-Healthcare for Maintaining Auditability and Privacy of Medical Reports

Amruta S. Dhange
Department of Computer Science and Engineering
WIT, Solapur

R.V. Argiddi
Department of Computer Science and Engineering
WIT, Solapur

ABSTRACT
The popularity of cloud computing has been increased exponentially as it provides different services depending on cost. To have privacy in healthcare systems a method is proposed in this project. This project offers options as well as economical key management, privacy-preserving knowledge storage, and retrieval, particularly for retrieval at emergencies, and auditability for misusing health knowledge. A method is projected to integrate key management from pseudorandom range generator for unlinkability, a secure classification methodology for privacy protective keyword search that hides each search and access patterns supported redundancy, and integrate the thought of attribute primarily based secret writing with threshold linguistic communication for providing role-based access management with auditability to forestall potential misconduct, in each traditional and emergency cases. The proposed method will also detect unethical distribution of health data, and identify possible sources of leakage.

Keywords
Auditability, Unlinkability, Pseudorandom range

1. INTRODUCTION
Instant access to personal health data enables advance healthcare services, which can improve quality of life, and adds more days in life by assisting timely treatment in medical emergencies. 24/7 accessible electronic healthcare systems play's very important role in our daily life. Healthcare services supported by mobile devices, such as home care and remote monitoring, allow patients to retain their living style and cause minimal interruption to their daily activities. Hence, it significantly reduces the hospital occupancy, only allowing patients with higher need of in-hospital treatment. Though these e-healthcare systems are increasingly popular, a large amount of personal data for medical purpose are involved, and also people live with the fear, that they would completely lose control over their personal information once it get uploaded on internet.

According to the government survey, in past 2 years around eight million patients' e-health data was leaked. Such leakage of e-health data can lead to, employer may decide not to hire someone with certain diseases or insurance company will not provide life insurance knowing the disease history of a patient. Despite the dominant importance, privacy problems aren't self-addressed adequately at the technical level and efforts to stay health knowledge secure have usually fallen short. This can be as a result of protective privacy within the computer network is considerably tougher. Hence it need a solution for viable protocols, architectures, and systems assuring privacy and security to protect sensitive and personal digital information. Adopting external data storage and computational tasks becomes a popular trend as we enter the cloud computing era. For e-healthcare payers such as medicare payers, insurance companies, municipalities, and self-insured employer health plans, the company's total claims capture and control (TC3) provides claim management solutions. To process sensitive health information the TC3 uses Amazon's EC2 cloud. Adopting the computation to the cloud saves, TC3 from buying and maintaining servers, and allows TC3 to take advantage of Amazon's expertise to process and analyze data faster and more efficiently. The cloud-assisted mobile health networking [1] is impressed by the ability, flexibility, convenience, and value potency of the cloud-based data/computation outsourcing paradigm. Users have a tendency to introduce the non-public cloud which might be thought of as a service offered to mobile users.

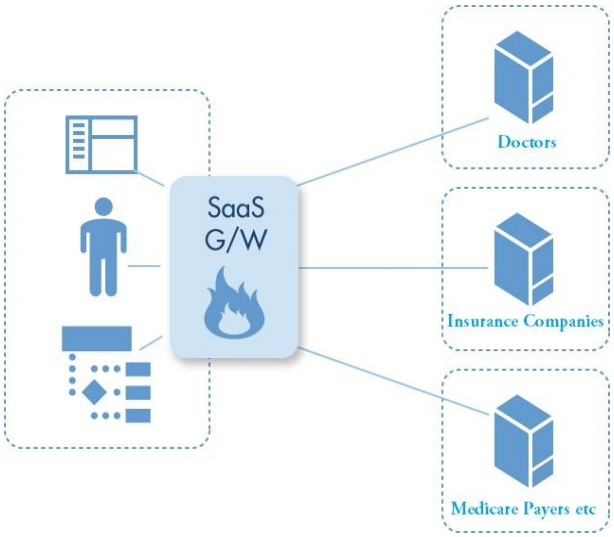


Fig 1: SaaS Service Model

The proposed solutions are built on the service model shown in Fig. 1. By using the infrastructure of the public cloud providers (e.g., Amazon, Google), a software as a service (SaaS) provider provides private cloud services. Mobile users send data processing tasks to the private cloud and this private cloud stores the processed results on the public cloud. The implementation of practical privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving mobile users with lightweight tasks, supported by cloud-assisted service model.

2. RELATED WORK
W.B.Lee and C.D. Lee, give solution, the trusted server is able to access the health data at any time, which could be a privacy threat[2]. Also [3] the work of C. C. Tan, shows a technical realization of the role-based approach, proposed scheme that failed to achieve privacy protection in the storage server learns which records are from which patient to provide results to a querying doctor.

The concept of patient-controlled encryption (PCE) such that health related data separated into a hierarchy of smaller piece of information which will be encrypted using the key which is under the patients' control. They gave a symmetric-key PCE for fixed hierarchy, a public-key PCE for fixed hierarchy, and a symmetric-key PCE for flexible hierarchy from RSA[4].

A system utilizes multi authority attribute-based encryption (ABE) for fine-grained access control. Their designed framework allows break-glass access via the use of "emergency" attributes. However, their is a ambiguity that who is responsible to create a powerful decryption key corresponding to this attribute in practice[5][6].

M.C.Mont, describes an innovative technical solution in the area of secure messaging that exploits identifier-based encryption (IBE) technology. It provides facility against a similar approach based on traditional cryptography and PKI. It discusses a few open issues. Their main contribution is a practical solutions based on IBE technology. A secure transmission system based on IBE has been fully implemented and it is currently used in a trial with a UK health service organization [7].

P. RayandJ. Wimalasiri, proposed a model of "proof of retrieve ability", where spot-checking as well as error-correcting codes have been used for ensure both "possession" as well as data files "retrieve ability" on archive service systems. Though the existing systems gives verification of integrity for various systems of data storage, the issue resulting to support public auditability as well as data dynamics is not fully addressed[8] .

G. Ateniese, R. Curtmola, B. de Medeiros, and D. Davis, pointed out the importance and unique challenges of medical information privacy, and the fixing privacy breach facts that resulted from insufficient supporting technology. MIPA that sought to develop privacy technology and privacy-protecting environment to facilitate the development of a health information system, in which patients can actively protect their personal information. [9]

J.Sun,X.Zhu,C.Zhang,andY.Fang, states that the privacy-preserving health data storage is studied, where patients encrypt their own health data and store it on a third-party server. Also backup mechanisms in this paper for emergency access rely on a process that the patient trusts whose availability cannot be guaranteed at all times. [10]

L. Zhang, G. J. Ahn, and B. T. Chu, proposed delegation framework addresses the issue of how to advocate selective information sharing in role- based systems while reducing the risks of unauthorized access. Wiederhold et al.[24] proposed a centralized solution to assign a security officer the responsibility to manage sharing of sensitive information. They formalized the role of a security officer who has responsibility to assure that no appropriate information can leave an enterprise domain. But under the healthcare environment, the patient's document sharing tends to be very dynamic and often ad hoc. Hence, this centralized management approach is not suitable to the healthcare domain because the workload on such an officer will be overwhelming. [11]

3. PROPOSED WORK

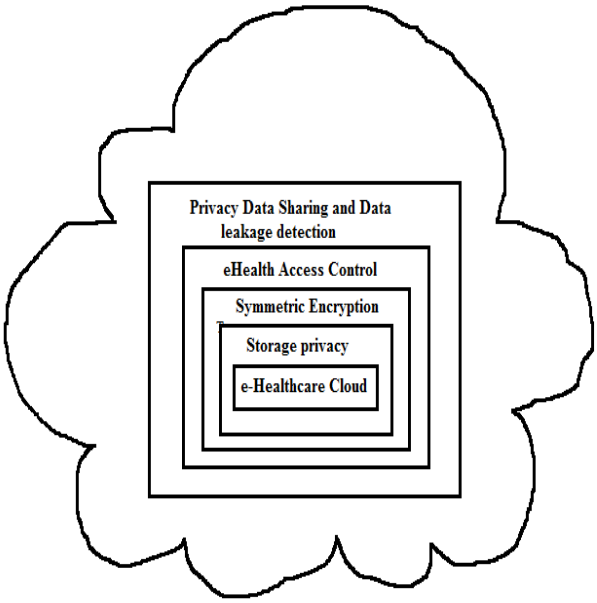
The aim of this paper is to provide flexibility, convenience, and cost efficiency of the cloud-based data/computation outsourcing paradigm. This paper introduces the private cloud which can be considered as a service offered to web users. The proposed solutions are built on the service model shown in Fig. 1. By using the infrastructure of the public cloud providers (e.g., Amazon, Google), a software as a service (SaaS) provider provides private cloud services. Mobile users send data processing tasks to the private cloud and this private cloud stores the processed results on the public cloud. The implementation of practical privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving mobile users with lightweight tasks, supported by cloud-assisted service model. This work also provides a mechanism that can detect whether users' health data have been illegally distributed, and identify possible source(s) of leakage (i.e., the authorized party that did it)

4. DESIGN AND ARCHITECTURE

Cloud computing is mechanism used to store and access data from anywhere and anytime. As numbers of cloud users are enormous, there is need to secure the data using different encoding and decoding technique.

The health data can be stored at anytime from any location. The information transformation from any testing lab to doctor is time consuming and it may be liable to vulnerability. So to have diagnosis and treatment in time, a fast process is required, our proposed work can become best alternative for traditional method of medical data transfer.

Modules of project



4.1 Storage Privacy

The user can be associated with the storage and retrieval process, i.e., these processes should be anonymous. Unauthorized parties should not be able to link more than one data files to profile a user. It indicates that the file identifiers should appear random and leak no useful information. Public Storage only collects that information from user which is necessary for providing the service and information that will be interested. The following three categories of information will be collected from user: (a) Personally Identifiable Information; (b) Non-Personal Information; and (c) Passive Anonymous Information. In this Privacy Policy all these three categories are collectively referred to as "Information".

4.2 Symmetric Encryption

The Secret sharing needs to be performed once and for all, and the ABE encryption of the shares needs to be performed only for a limited number of general roles. Encrypting a

message does not guarantee that this message is not changed while encrypted. Hence often a message authentication code is added to a ciphertext to ensure that changes to the ciphertext will be noted by the receiver. Message authentication codes can be constructed from symmetric ciphers.

The shared secret is either shared beforehand between the sender and receiver, in which case it can also be called a pre-shared key, or it is initiated at the start of the communication session by using a key-agreement protocol, for-instance using public-key cryptography such as Diffie-Hellman or using symmetric-key cryptography such as Kerberos

4.3 eHealth Access Control

The access control is achieved by our ABE-control threshold signing scheme, where the expensive ABE operations are only used for encrypting small values and the majority of data encryption is fulfilled by efficient symmetric key scheme. the access structure is specified. This will show that cryptosystem gives a powerful framework for encryption with fine-grained access control for applications. Fine-grained access control systems facilitate granting different access roles to a set of users and allow flexibility in specifying the access rights of individual users.

4.4 Privacy Data Sharing

It is the ability for sharing the same data resource with multiple applications or users. With this module the data are stored in one or more servers in the network and this module also provide some software locking mechanism to prevent the same set of data from being changed by two people at the same time. The primary feature of a database management system is data sharing. The privacy protection for e-health data concentrate on the framework design including the demonstration of the significance of privacy for e-health systems, the authentication based on existing wireless infrastructure

4.5 Data Leakage Detection

The ability to find out fraud and illegal violence of e-healthcare data of patients. It creates a threaten for the inside intruders that they can track if they violate the data protection. This can be achieve using hiding the chain of user list who were involve in data transfer inside the file itself.

4.5.1 Steganography

The objective of using steganography is to hide the chain of user names who involved in file sharing within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another".

Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements [12]

- The cover media(*C*) that will hold the hidden data
- The secret message (*M*), may be plain text, cipher text or any type of data
- The stego function (*Fe)* and its inverse (*Fe-1*)
- An optional stego-key (*K*) or password may be used to hide and unhide the message.
- The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media (*S*).

The schematic of steganographic operation is shown below.

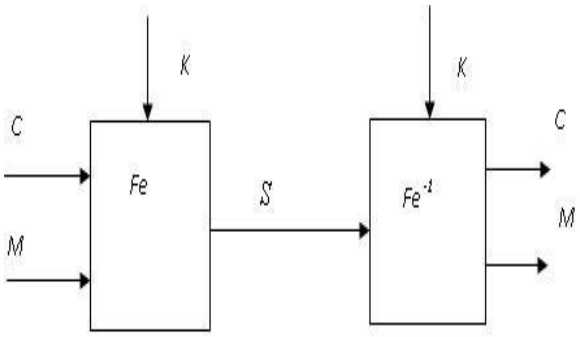


Fig 3: The Steganographic operation

5. CONCLUSION

The proposed work can be useful to the people who not gave time for heath diagnosis due to time factor now day to day life. It also ensures the privacy and data leakage detection, so patients can use this e-healthcare services fearlessly. Also this method provide mobile friendly interface which can be used by any normal person now a days.

6. SCOPE

Cloud computing is mechanism used to store and access data from anywhere and anytime. As numbers of cloud users are enormous, there is need to secure the data using different encoding and decoding technique.The health data can be stored at anytime from any location. The information transformation from any testing lab to doctor is time consuming and it may be liable to vulnerability. So to have diagnosis and treatment in time, a fast process is required, proposed work can become best alternative for traditional method of medical data transfer.

7. REFERENCES

[1] "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, JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. 18, NO. 2, MARCH 2014

[2] 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.

[3] C. C. Tan, H.Wang, S. Zhong, and Q. Li, "Body sensor network security: An identity-based cryptography approach," in *Proc. ACM Conf. Wireless Netw. Security*, Apr. 2008, pp. 148–153.

[4] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronicmedical records," in *Proc. ACM Workshop Cloud Comput. Security*, 2009, pp. 103–114.

[5] C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key aggregate cryptosystem for scalable data sharing in cloud storage," *IEEE Trans. Parallel Distrib. Syst.*,vol.99,no.PrePrints,p.1,2013.Available:http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.112

[6] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 121–130.

[7] 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.

[8] 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, pp. 86–4689.

[9] G. Ateniese, R. Curtmola, B. de Medeiros, and D. Davis, "Medical information privacy assurance: Cryptographic and system aspects," presented at the 3rd Conf. Security Commun. Netw., Amalfi, Italy, Sep. 2002.

[10] J. Sun, X. Zhu, C. Zhang, andY. 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] 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, pp. 125–134.

[12] Steganographic Techniques and their use in an Open-Systems Environment- Bret Dunbar, The Information Security Reading Room, SANS Institute 2002 http://www.sans.org/readingroom/whitepapers/covert/677.php

[13] L. Zhang, G. J. Ahn, and B. T. Chu, "A rule-based framework for role based delegation and revocation," ACM Trans. Inf. Syst. Security, vol. 6, no. 3, pp. 404–441, 2003.

[14] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing. Extended abstract in CRYPTO 2001," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.

[15] 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.

[16] X. Liang, R. Lu, L.Chen, X. Lin, andX. Shen, "PEC:A privacy-preserving emergency call scheme for mobile healthcare social networks" *J. Commun. Netw.*, vol. 13, no. 2, pp. 102–112, 2011.

[17] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attributed-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[19] 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.

[20] N. Cao, Z. Yang, C.Wang, K. Ren, andW. Lou, "Privacy-preserving query over encrypted graph-structured data in cloud computing," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 393–402.

[21] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on PHI in e-healthcare systems," Adv. Health Inform. Conf., pp. 1–5, Apr. 2010.

[22] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on PHI in ehealthcare systems," Adv. Health Inform. Conf., pp. 1–5, Apr. 2010.

[23] Y. C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. 3rd Int. Conf. Appl. Cryptogr. Netw. Security, 2005, pp. 442–455.

[24] G. Wiederhold, M. Bilello, V. Sarathy, and X. Qian: "Protecting Collaboration"; Proceedings of the NISSC'96 National Information Systems Security Conference, pages 561-569. Oct. 1996.