MediCloud: Cloud Computing Services to Health Sector

Amit S. Pawade
Professor
Department of Computer Science and Engineering
NBN Sinhgad College of Engineering, Solapur

Rajan S. Jamgekar
Professor
Department of Computer Science and Engineering
NBN Sinhgad College of Engineering, Solapur

ABSTRACT

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. 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. 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 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. Despite the paramount importance, privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short. This is because protecting privacy in the cyberspace is significantly more challenging. Thus, there is an urgent need for the development of viable protocols, architectures, and systems assuring privacy and security to safeguard sensitive and personal digital information.

Keywords

Access control, auditability, eHealth, privacy, cloud computing.

1. INTRODUCTION

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.

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 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. Despite the paramount importance, privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short. This is because protecting privacy in the cyberspace is significantly more challenging. Thus, there is an urgent need for the development of viable protocols, architectures, and systems assuring privacy and security to safeguard sensitive and personal digital information. Outsourcing data storage and computational tasks becomes a popular trend as we enter the cloud computing era. A wildly successful story is that the company's total claims capture and control (TC3) which provides claim management solutions for healthcare payers such as medicare payers, insurance companies, municipalities, and self-insured employer health plans.TC3 has been using Amazon's EC2 cloud to process the data their clients send in (tens of millions of claims daily) which contain sensitive health information. Outsourcing 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 proposed cloud-assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the cloud-based data/computation outsourcing paradigm. We have introduced 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

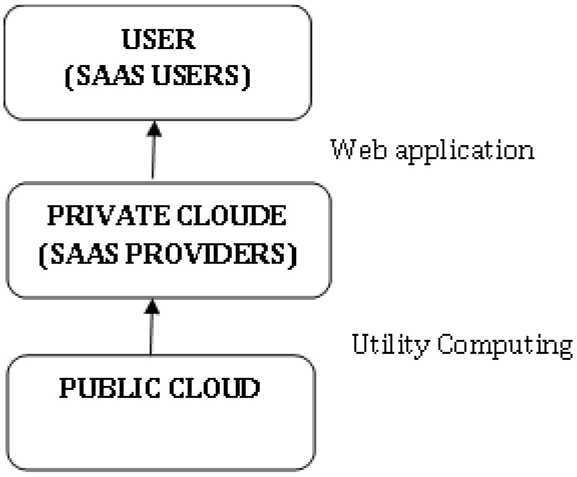

Fig. 1. SaaS service model

2. RELATED WORK

Role-based access control is an enabling technology for managing and enforcing security in large-scale and enterprise wide systems. The basic notion of RBAC is that permissions are associated with roles, users are assigned to appropriate roles, and users acquire permissions by being members of roles. Users can be easily reassigned from one role to another. Roles can be granted new permissions. And permissions can be easily revoked from roles as needed. This greatly simplifies security management [24]. Constraints can apply to relations and functions defined in an RBAC model to establish higher-level organizational policy.

Thomas et. Al formulated team-based access control (TMAC) [26] and task-based access control (TBAC) [25] as active security models. This approach models access control from a context oriented perspective than the traditional subject-object one .TMAC and TBAC are aware of the context information associated with an ongoing activity. Thus, they provide a natural way to control access for collaborative activities in teams and workflows. However, We argue that TBAC modes are specific configurations of role-based access control, where context information can be viewed as constraints.

G. Ateniese, R. Curtmola applied general principles of security in medical information field, a number of unique characteristics of the health care business environment suggest a more tailored approach. Electronically-managed information touches almost all aspects of our daily life in modern society. Cryptographic techniques can be used to assure that sensitive information is kept secure and, in general, to protect communication systems. The communication infrastructure is made secure, all privacy problems will not disappear. While making the Internet as secure as possible is necessary for privacy, it is not sufficient in and of itself. Security is not synonymous with privacy. The intelligence and financial industries are likely to be used for criminal purposes, such as the sale of military secrets or fraud, respectively. With medical information such breaches and uses may be more insidious, and the damages less over. Advantage of this technique is this technique improves the security and privacy of electronic medical data but it results decrease in performance and increase in cost [20].

J. Sun, C. Zhang, Y. Zhang proposed vehicular ad hoc network (VANET) which can offer various services and benefits to users and thus deserves deployment effort. Attacking and misusing such network could cause destructive consequences. It is therefore necessary to integrate security requirements into the design of VANETs and defend VANET systems against misbehavior, in order to ensure correct and smooth operations of the network. The most related works are on the design of privacy-preserving schemes. Raya and Hubaux investigated the privacy issue by proposing a pseudonym based approach using anonymous public keys and the public key infrastructure (PKI), where the public key certificate is needed, giving rise to extra communication and storage overhead. The authors also proposed three credential revocation protocols tailored for VANETs, , considering that the certificate revocation list (CRL) needs to be distributed across the entire network in a timely manner. VANET security system achieves privacy, traceability to the great extend. Functionalities are realized by the pseudonym-based technique.

ID-based cryptosystem facilitates us to design communication and storage efficient schemes. Drawback of this system is VANET settings are made in theoretical manner not in reality [21].

J. Sun, X. Zhu, C. Zhang proposed electronic health record system which is more efficient and less error -prone. Privacy concern is arguably the major barrier that hinders the deployment of electronic health record (EHR) systems which are considered more efficient, less error-prone, and of higher availability compared to traditional paper record systems. Patients are unwilling to accept the EHR system unless their protected health information (PHI) containing highly confidential data is guaranteed proper use and disclosure, which cannot be easily achieved without patients' control over their own PHI. EHR systems are not adopted by the majority of healthcare systems. Statistical results of the actual adoption rate of HER in US medical systems and the references therein. Among all the barriers to the implementation of EHR systems, privacy and security concerns on patients' medical records are arguably most dominating. Records stored in a central server and exchanged over the Internet are subject to theft and security breaches. A secure EHR system is used to protect patient privacy and enable emergency healthcare. The technique is resilient to various attacks and satisfies the security requirements. It maintains good balance between security and efficiency. The drawback of this method is cell phone would suffice due to the low complexity of the retrieval protocol [23].

L. Guo, C. Zhang, J. Sun developed eHealth systems which 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. The widely deployed electronic health (eHealth) system has changed people's daily life other than traditional paper based system for its extraordinary advantages, such as more efficiency, high accuracy and broader availability However, privacy concern is arguably the major barrier that hinders the development of electronic health record (EHR) stored in a public storage with direct connection to a network. The most relevant work is Li.et al. which considers a privacy-preserving personal profile matching scheme for mobile social networks, which implements secure multi-party computation based on polynomial secret sharing. Their scheme is fully distributed, where users share their attributes among a group of valid users using Shamir secret sharing scheme., they design a secure friend discovery scheme based on secure dot product protocol by using homomorphic encryption. Multiple papers address the problem of Secure Private Intersection (PSI), which is related to the highest privacy level in our proposed system. The drawback of this method is it is non-interactive proof system as the basic building block [22].

M.C.Mont, P.Bramhall, and K.Harrison 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. Their main contribution is a practical solutions based on 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. [Related 000]

3. DESIGN AND ARCHITECTURE OF SYSTEM

This implementation consists of four modules,

1. Storage Privacy
2. Symmetric Encryption
3. eHealth Access Control
4. Privacy Data Sharing

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 multiple data files to profile a user. It indicates that the file identifiers should appear random and leak no useful information. Public Storage only collects information from you that is necessary for us to provide service and information that we believe will interest you. We collect the following three categories of information from you: (a) Personally Identifiable Information; (b) Non-Personal Information; and (c) Passive Anonymous Information. All three of these categories are collectively referred to as "Information" in this Privacy Policy.

•To provide a report to our advertisers or business partners that tells them who responded to a particular offer to facilitate the fulfillment of an order that you have made with an advertiser or business partner;

•To customize, personalize, analyze, evaluate, adjust and improve the Site and our services to meet your needs and expectation and those of our business partners;

•To describe our customer audience, products and services;

•To develop partnerships with third parties to offer products or services which we believe will interest our customers;

•To anonymize or aggregate PII for various purposes, such as market or traffic flow analysis and reporting; and

•To process job applications and for recruitment purposes.

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 cipher text to ensure that changes to the cipher text will be noted by the receiver. Message authentication codes can be constructed from symmetric ciphers.

The shared secret is either shared beforehand between the communicating parties, in which case it can also be called a pre-shared key, or it is created 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

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 secret values and the majority of data encryption is fulfilled by efficient symmetric key scheme. the access structure is specified. We will show that this cryptosystem gives us a powerful tool for encryption with fine-grained access control for applications such as sharing audit log information. Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users.

4. Privacy Data Sharing

It is the ability to share the same data resource with multiple applications or users. It implies that the data are stored in one or more servers in the network and that there is some software locking mechanism that prevents the same set of data from being changed by two people at the same time. Data sharing is a primary feature of a database management system. 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

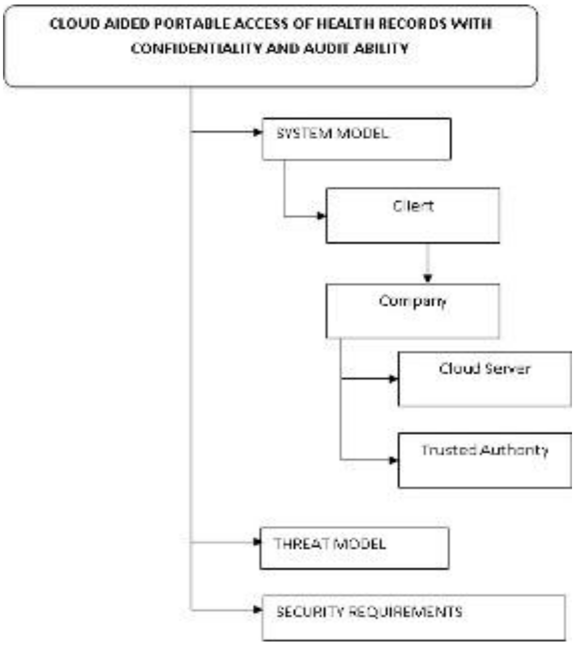

Fig 2. System Architecture Design

4. RESULT AND DISCUSSION

The technique is implemented using Java language and MYSQL is used as database.

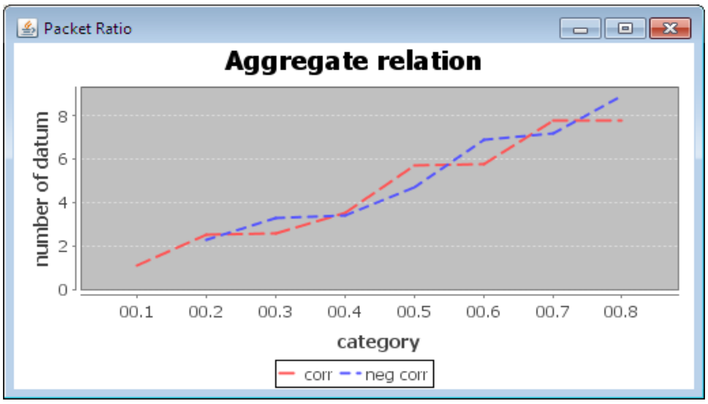

Fig 3 Aggregate Relation Graph

Health data stored on clouds is stored in encrypted form and index based searching method is used to retrieve the same.

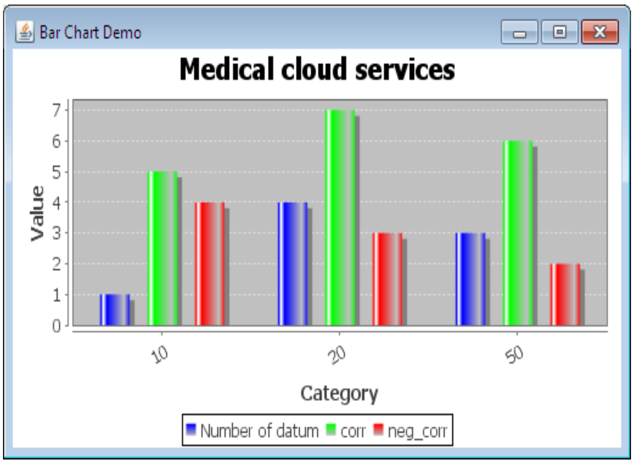

Fig 4. Medical Cloud Service Graph

This technique results in accurate and efficient method with small data sets. Private cloud does not ensure the security but it gives confidence if encryption method is associated with techniques.

5. CONCLIUSION

Our method provides privacy into mobile health systems with the assistance of the personal cloud. We have a tendency to provide an answer for privacy-preserving knowledge storage by desegregation based key management for un-link ability, a hunt and access pattern concealment theme supported redundancy, and a secure compartment allegation technique for privacy-preserving keyword search. We also investigated techniques that give access management and auditability of the licensed parties to forestall misbehavior, by combining ABE-controlled threshold linguistic communication with role-based secret writing. As future work, we decide to devise mechanisms which will notice whether or not users' health knowledge are lawlessly distributed, and establish doable source(s) of escape.

6. REFERENCES

[1] Sherman S. M. Chow and Pan Li, Member, IEEE ,"Cloud-Assisted Mobile-Access of Health Data with Privacy and Audit ability", IEEE, Journal of Biomedical and Health Informatics, VOL. 18, NO. 2, March 2014

[2] P.Rayand, J.Wimalasiri,"The need for technical solutions for maintaining the privacy of EHR," in Proc. IEEE 28thAnnu.Int.Conf.,NewYorkCity, NY, USA, Sep. 2006, pp. 4686–4689

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

[4] J. Sun, X. Zhu, and Y. Fang, "Preserving privacy in emergency response based on wireless body sensor networks," in Proc. IEEE Global Telecom- mun. Conf., Dec. 2010, pp.

[5] 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.

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

[7] 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.

[8] C. Wang, K. Ren, S. Yu, and K. Urs, "Achieving usable and privacy- assured similarity search over outsourced cloud data," in Proc. IEEE Conf. Comput. Commun., Mar. 2012, pp. 451–459.

[9] M.Li, S.Yu,Y. Zheng, K.Ren and W.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.

[10] N.Cao, Z.Yang,C.Wang,K.Ren,and W.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.

[11] D.Song, D.Wagner,andA.Perrig,"Practical techniques for searching on encrypted data," in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.

[12] A.Pingley, W.Yu,N.Zhang, X.Fu and W.Zhao, "CAP:Acontext-aware privacy protection system for location-based services," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., 2009, pp. 49–57.

[13] 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.

[14] 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.

[15] 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.

[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attributed-based encryp- tionforfine-grained access control of encrypted data,"inProc.ACMConf. Comput. Commun. Security, 2006, pp. 89–98.

[17] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption:Ensuring privacy o felectronic medical records,"inProc.ACM Workshop Cloud Comput. Security, 2009, pp. 103–114.

[18] M. Chase and S. S. M. Chow, "Improving privacy and security in multi- authority attribute-based encryption," in Proc. ACM Conf. Comput. Com- mun. Security, 2009, pp. 121–130.

[19] 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.

[20] 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

[21] 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

[22] 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

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

[24] Ravi S. Sandhu{, Edward J. Coynek, Hal L. Feinsteink and Charles E. Youmank "Role-Based Access Control Models" IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47.

[25] LONGHUA ZHANG, GAIL-JOON AHN, and BEI-TSENG CHU "A Rule-Based Framework for Role-Based

Delegation and Revocation" ACM Transactions on Information and System Security, Vol. 6, No. 3, August 2003, Pages 404–441.

[26] Weigang Wang, "Team-and-Role-Based Organizational Context and Access Control for Cooperative Hypermedia Environments"