A novel patient centric framework for secure sharing of confidential health records in cloud computing

SUSMITHA MANDAVA*
Student
Dept of Computer Science Engineering
Bharath University, Chennai, India
Selaiyur– 600073
susmithacse.m@gmail.com

Mrs.ANURADHA
Assistant Professor
Dept of Computer Science Engineering
Bharath University, Chennai, India
Selaiyur - 600073
anuratha@gmail.com

Abstract —

In the current era even however there is a huge conversion in healthcare expertise, still patients are suffering from prevalent syndromes. Satisfying and providing high safety to enormous patient's trusted fitness info is becoming stimulating day by day. Now a days there is\ an emergence of web based system called Delicate Fitness Record (DFR) which is subcontracted to Cloud Calculating providers. Security of DFR's mainly encompasses of privacy and confidentiality. However there is a huge privacy concerns as DFRs could be unprotected to cloud deducting providers servers and from being viewed to illegal machinists without patients agreement. With this paper, we familiarize a original patient-centric outline called quality grounded encryption for statistics access control to DFRs stored in cloud servers. To achieve fine-grained data access control for DFRs, we use the aspect grounded encryption instrument to encrypt each patient's individual fitness file. Dissimilar from previous works in secure data subcontracting, we mostly emphasis on the several data possessor concept. In this scheme we segregated the users in the DFR scheme into multiple safety domains that decreases the key administration difficulty for owners and users. In this mechanism we assure patient privacy and concurrently exploiting multi-authority. Additionally our mechanism enables dynamic modification of access policies to sustain efficient on-demand revocation of user/attribute and break-glass access under crisis situation. With our Unique Patient Centric Outline we demonstrate the effectiveness, of our outline with high degree of safety in addition to scalability by presenting extensive analytical and investigational results.

Keywords- Trusted patient's fitness archives, Scattered figuring, statistics privacy, adequate crumbed entrée device, Statistics Regular Encryption

I. INTRODUCTION

Delicate Fitness care has an importance itself in this modern age, and people are in extreme need of an organized tool to look after the Health issue of the particular individual.
In current age, Delicate Fitness Record (DFR) has come forward with a rational framework which helps and allows a patient to keep the record of personal health information on web. The web is strong platform designed to retrieve and share the information about the health more efficiently. It works like news feed. A particular patient can share his issue with lot of other similar kind of patients including health information by health care providers. There has been taken special case of confidentiality risks about the patient. We have healthcare regulations such as HIPAA which is recently amended to incorporate business associates. A DFR file should only be accessible to the users only have been given a decrypted key. We have organized DFR a secure framework with particular information and user friendly options.
We also use MultiAuthority in public domain to improve the security and make sure of all the things are in control. Also there is an option to calculate the complexity and scalability of our proposed secure DFR sharing solution.

II. RELATED WORK

This paper is predominantly associated to works in cryptographically enforced access control for outsourced data and attribute based encryption.

Acceptable crumbed Statistics Access Control for Aspect Grounded Encryption

Managing online Confidential personal health record in the form centralized repository enables patients to store, access, share their data to wider users, including physicians, nurses, healthcare providers, family members or friends. Ever since the Cloud computing came into existence, it becomes imperative for DFR Service providers to transfer their DFR confidential and privacy data of patients into the Cloud Servers, which drastically reduce the operational cost and time. However, one of the limitations of storing DFRs in the cloud server is that patients lose physical control to confidential personal health data, which prompts each patient to encrypt their DFR data prior to uploading to the cloud servers. The limitation of encryption is that it is challenging to achieve fine-crumbed access control to DFR data in a scalable and efficient way because each patient's DFR data should be encrypted so that it is scalable with the number of users having access. Moreover, since there are multiple patients in a DFR system and every patient would encrypt their DFR files using a different set of cryptographic keys, it is quite important to decrease the key.

© 2014 IJAIR. ALL RIGHTS RESERVED

With this paper, we propose a novel framework to enable fine-crumbed dtata access control for DFRs by leverage aspect based encryption techniques to encrypt each patient's DFR data. In order to shrink the key distribution complexity, we also segregate the entire system into multiple security domains. In this system each domain manages only a subset of the users. By this way, each patient has full control over their own privacy and confidential data which results abruptly decrease in key management complexity. Our Proposed framework enables dynamic modification of access policies to sustain efficient on-demand revocation of user/attribute and break-glass access under crisis situation.

Safeguarding the Electronic Trusted Health archives

In the current era Information technology is playing a key role in healthcare industry to deliver high quality, increased productivity, cost-effective and personalized healthcare services. The latent aspects of electronic confidential health records are easy and universal accessibility to patient's medical histroy, and providing opportunities for new business models. In this paper, we spot out several limitations of current e-health solutions and standards where current system does not address the client platform security. This is a crucial aspect for the overall security of e-health systems.To fill this gap, we present security architecture for establishing privacy domains in e-health infrastructures.Our projected exposition provides security to client platform as well as aptly combines this with security concepts of network. Moreover, we discuss additional open problems and research challenges on security, privacy and usability of Electronic Confidential Health records.

Searching encrypted trusted health archives in cloud computing using Secret keyword

In the current era, cloud computing becomes a most conventional technology. The cloud computing holds several advantages as more secure and less expensive then tradional computing networks. Due to which many healthcare organizations have adopted this platform which includes health care professionals, physician practices and nurses. In cloud computing, Application services run on remote-hosted platforms as well as on a client (computer or mobile device). Access to Confidential health and clinical data is delivered through terminal services technology or virtual private networks, giving the illusion of a truly web-based application or thin client. While those data may contain sensitive personal information, the cloud servers

Preserving and accessibility automated medical archives

A patient's medical records are generally fragmented across multiple treatment sites, posing an obstacle to clinical care, research, and public health efforts.1 The information technology has provided immense technical infrastructure through internet by accessing of patients e-medical records up on which longitudinal medical records that can be integrated across sites of care. The felxibillity about the ownership and the structural choice of these records will have deep impact on the confidentiality, privacy and accessibility of patient information. Currently there are webbased medical records systems are developed and widely used across the globe. The information technology is playing a vital role in unifying the contrasting histyory of a patient's medical record may actually threaten the accessibility of the patient's health data and compromise patients' confidentaility and privacy. With this article we propose development of webbased medical record systems by introducing two doctrines and six desirable characteristics. We have choosen key clinical aspects of healthcare industry and illustrate that how such system could be developed and used clinically.

Secrecy of automated medicinal histories

We explore the challenge of preserving patients' privacy in electronic health record systems. The security in such systems should be enforced via encryption as well as access control. In addition to above said, we also argue for approach that enable patients to store and generate encryption keys, as a result the patients' privacy is protected. The functionality of the system would be interfered by encryption which becomes the standarad argument. However, we demonstrate to build proficient system that permit patients, not only allocate partial access rights with others, but also searches over their respective records. We formalize the Patient Controlled Encryption scheme, requirements and bestow several instantiations, based on existing cryptographic primitives and protocols, to attain a different set of properties.

For cloud-based DFR systems, we illustrated our novel patient-centric secure data sharing framework.

In the below Table 1.the main notations are summarized.

Table 1 – Frequently Used Notations

$\mathcal{U}_D, \mathcal{U}_R$	The attribute universes for data and roles
$\mathcal{T}, L(\mathcal{T})$	A user access tree and its leaf node set
A_k^C	Attributes in the ciphertext (from the kth AA)
A_k^u	User u's attributes given by the kth AA
A, a	An attribute type, a specific attribute value of that type
$\mathcal{P}$	Access policy for a PHR document
P	A key-policy assigned to a user
MK, PK	Master key and public key in ABE
SK	A user's secret key in ABE
$rk_j^{(k)}$	Proxy re-key for attribute j and version k

© 2014 IJAIR. ALL RIGHTS RESERVED

III. PROPOSED TECHNIQUE

In this paper we propose a Novel patient-centric framework which not only boosts up patient's long term medication goal but also helps patients several kinds of medical diagnoses. Our Proposed technique is a cluster of mechanisms which efficiently access data and respective controls to Patients called Delicate Fitness Record (DFR) which resides in cloud servers. In order to accomplish our primary goal of Fine crumbed Data Access Control for (DFR) we influenced aspect based encryption scheme to encrypt individual DFR File. By using aspect based Scheme entire access polices are articulated based on the attributes of DFRs. Our framework facilitates patient to share their DFRs to various users by encrypting the file under patients set of attributes.

The Novel Patient Centric framework is illustrated in below Fig. 1, which consists of multiple SDs, Owners, Personal Aas and users.

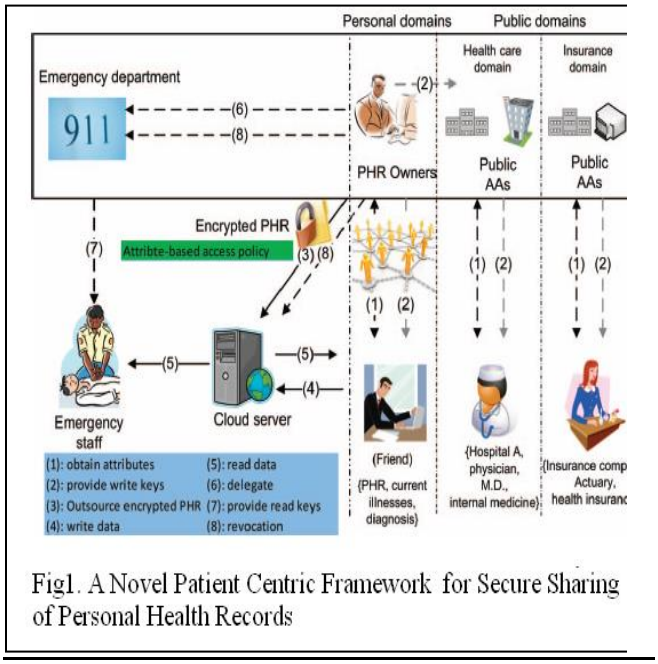

Fig1. A Novel Patient Centric Framework for Secure Sharing of Personal Health Records

efficiency. Revocation of a personal domain user's access privileges. These can be initiated through the DFR owner's client application in a similar way.

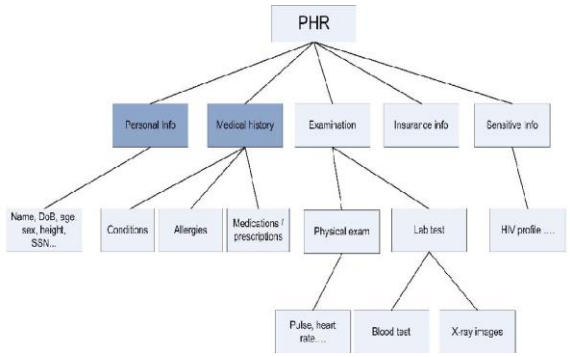

Fig. 2. The attribute hierarchy of files—leaf nodes are atomic file categories while internal nodes are compound categories. PSD's data readers have access to Dark boxes.

Table 2
Sample Secret Keys and Key-Policies for three Public users in the Health care Domain

Attribute authority	AMA		ABMS	AHA
Attribute type	A P f n	A L n t tu	A_3 Medical specialty	A_4 Organization
A u 1	Physician	M.D.	Int n l m d n	Hospital A
A : user 2	Nurse	Nurse license	Gerontology	H ɻ t l I'
A u 3	Ph m t	Ph m l n	G n l	Pharmacy C
Key policies	1 ut f n	∧1 ut f n	1 ut f n_3	1 ut f n_4

IV. EXPERIMENTAL SETUP & RESULT

We have chosen JAVA as programming language and Database backup is in MYSQL with adjusting Tool Net beans IDE 7.0 to perform the operations in this application.

Our primary focal point was on the multiple data owner scenario for which segregated the users in the DFR system into manifold security domains which ultimately diminished the owners and users key management complexity.

With this paper, we associated the above gaps by proposing a amalgamated security framework for patient-centric sharing of DFRs with many users in a multi-domain and authority DFR system. Our proposed framework not only confined application level requirements of both public and personal use of a patient's DFRs but also allocates users' trust to multiple authorities which better replicates reality.

V. CONCLUSION

In this paper, a system has been designed to help a patient to keep the record of his daily fitness issues online on the cloud. This is more secure and easy to access on web. In this proposed system decryption key has also been maintained for the patient to keep the information confidential and access to the various users is an easy job to done, as well health care providers by this system.

© 2014 IJAIR. ALL RIGHTS RESERVED

VI. REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[2] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[4] "The Health Insurance Portability and Accountability Act,"http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp, 2012.

[5] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them" http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded," http://articles.latimes.com/2006/jun/26/health/heprivacy26, 2006.

[7] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287, Feb. 2001.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10, 2010.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[12] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010.

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryp- tion with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[14] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," 2009.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS'10), 2010

© 2014 IJAIR. ALL RIGHTS RESERVED