IJRRECS/June 2015/Volume-3/Issue-6/4161-4165 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A NOVEL PROPOSAL FOR ALLOCATION OF PERSONAL HEALTH DATA ON CLOUD SERVER

Mallela Nikhil[1], D.Swathi[2]

[1]M.Tech Student, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

ABSTRACT:

In our work we make an effort towards learning of a patient-centric and secure sharing of personal health records that are stored on semi-trusted server. The main objective of our work is to make available protected patient-centric personal health record access and resourceful key management at the same time. We present a novel attribute based encryption structure for secured patient-centric sharing of personal health records in a multi-domain cloud computing system with numerous users. For securing of personal health data that is stored on a semi-trusted server, we put into practice attribute based encryption as the most important encryption primitive. By means of proposed technique, patients can select and implement their own access policy for each personal health records file, and can revoke a user devoid of involving high transparency. To handle important challenges of management, we divide users in system into two domains such as public and personal domains. The framework which was introduced implements public as well as personal use of a patient personal health records, and share out user trust to numerous authorities. Our system handles a variety of types of applications needs of personal health data all together while incurring minimal key management transparency for owners and users in system.

Keywords: Patient-centric, Personal health records, Attribute based encryption, Key management, Cloud computing, Multi-domain, Access policy.

1. INTRODUCTION:

In literature there are quite a lot of works that has been using Attribute based encryption to recognize fine-grained access control intended for outsourced data. Moreover there is an increasing demand for application of attribute based encryption towards securing of electronic healthcare records [1]. Because of high cost for maintaining specific data centres, numerous services of personal health records are provided by the providers of third-party service. While it is motivating to contain efficient services of personal health records for each and everyone, there are a lot of security as well as confidentiality issues which could obstruct its extensive implementation. The most important concern is with reference to the patients that whether they could manage sharing of their personal health information, particularly when they are maintained on a third-party server which may not be completely trusted. Because of important significance of sensitive personal health information, third party storage servers are generally the targets of a variety of malicious behaviours which might lead to revelation of personal health information [2][3]. A service of personal health record as shown in fig1 allows a patient to generate and manage the personal information of health in single place all the way through web, which has made retrieval as well as sharing of medical information more resourceful. Our work is related to the works which are cryptographically enforced access control in support of outsourced data. A promising method would be to encrypt data earlier than outsourcing is frequently in conflict with scalability in personal health records system. In our work we propose a unified security structure for patient-centric sharing of personal health records in a multi-domain system with numerous users. The introduced framework confines public as well as personal use of a patient personal health records, and share out user trust to numerous authorities. The majority of conventional works do not distinguish among personal and public domains which have various attribute definitions and requirements of key management. By means of our method, patients can select and implement their own access policy for each personal health records file, and can revoke a user devoid of involving high transparency.

2. METHODOLOGY:

In our work we attempt to study patient-centric, and secure sharing of personal health records that are stored on semi-trusted servers. For protection of personal health data that is stored on a semi-trusted server, we implement attribute based encryption as the most important encryption primitive. The principal objective of our structure is to make available protected patient-centric personal health record access and resourceful key management simultaneously. We put forward a novel attribute based encryption structure for secured patient-centric sharing of personal health records in a multi-domain cloud computing system with numerous users. By means of attribute based encryption access policies are expressed on the basis of user attributes that permits a patient to share personal health data among a set of users by means of encrypting file, without knowing entire users list [4]. To deal with the important challenges of management, we divide users in system into two domains such as public and personal domains. The public domain consists of users who build access on the basis of their professional roles. For the most of traditional works do not distinguish among personal and public domains which have various attribute definitions, and requirements of key management. Our framework can handle various types of applications needs of personal health data at the same time while incurring minimal key management transparency for owners and users in system. The personal health record system has to support users from personal domain as well as public domains. For each personal domain its users are associated with a data owner, and they make access to personal health record on the basis of access rights assigned by owner [5]. While the set of users from public domain might be huge in size and irregular, system has to be extremely scalable, regarding difficulty in key management and storage.

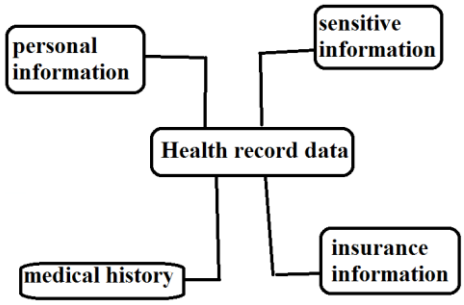

Fig1: An instance of health record data.

3. AN OVERVIEW OF PROPOSED NOVEL PATIENT-CENTRIC APPROACH:

For achieving of patient-centric personal health record sharing, an important necessity

is that each patient can manage the authorized persons who are to access her personal health documents. In our work the server was believed to be semi-trusted to be precise honest but curious which denotes that, the server will attempt to detect secret information in stored health record files as promising but they will honestly implement protocol in general. However, some users will moreover attempt to access the files beyond their privileges. We imagine a personal health record system in which there are numerous health record owners as well as users. The owners denote the patients who have complete control over their personal health record data such as they can create, handle, as well as remove it. There is a central server that belongs to service provider of personal health record that stores owner' personal health data. The most important goal of our structure is to make available protected patient-centric personal health record access and resourceful key management simultaneously. The important notion is to divide system into numerous public and personal domains. The personal health record system has to support users from personal domain as well as public domains. However the most of conventional works do not differentiate among personal and public domains which have a range of attribute definitions and requirements of key management. In both of these security domains, we make use of attribute based encryption to recognize cryptographically enforced, patient-centric personal health record access. In a public domain, multi-authority attribute based encryption is used, in which there are numerous attribute authorities each of which governs a disjoint subset of attributes. The public domain consists of users who build access on the basis of their professional roles. As the set of users from public domain might be huge in size and irregular, system has to be extremely scalable, regarding difficulty in key management and storage. Users in public domains obtain their attribute-based secret keys from attribute authority devoid of interacting with owners. Each data owner is a trustworthy authority of her own personal domain who manages secret keys as well as access rights of users in their personal domain. For each personal domain its users are connected with a data owner, and they make access to personal health record on the basis of access rights assigned by owner. Since public domain contains majority of users, it to a great extent reduces key management transparency for owners as

well as users. For personal domain, data attributes are described which refer to intrinsic properties of personal health record data. While the number of users in a personal domain is frequently small, it lessens burden for owner. When encrypting data for personal domain, all that owner needs to recognize is fundamental data properties [6].

4. CONCLUSION:

For securing of personal health data that is stored on a semi-trusted server, we execute attribute based encryption as the most important encryption primitive. We recommend a unified security structure for patient-centric sharing of personal health records in a multi-domain system with numerous users. By attribute based encryption access policies are conveyed on the basis of user attributes that permits a patient to share personal health data among a set of users by means of encrypting file. By our technique, patients can choose and employ their own access policy for each personal health records file, and can revoke a user devoid of involving high transparency. To manage essential challenges of management, we divide users in system into two domains such as public and personal domains. The system confines public as well as personal use of a patient personal health records, and share out user trust to numerous authorities. Our personal health record system contains numerous health record owners as well as users and can hold various types of applications needs of personal health data at the same time while incurring minimal key management transparency for owners and users in system.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

[6] 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.