International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : 10.32628/CSEIT1952233

An Efficient Key Management for Medical Data Access Using ABE

S. Keerthana[1], A. Ponmani[1], R. Pragathe[1], R. Udhaya[1], P. Parthasarathi[2], Dr. N. Suguna[3]

[1]B. E. Scholar, Computer Science and Engineering, Akshaya college of Engineering and Technology, Kinathukadavu, Tamil Nadu, India
[2]Assistant Professor, Computer Science and Engineering, Akshaya college of Engineering and Technology, Kinathukadavu, Tamil Nadu, India
[3]Professor, Computer Science and Engineering, Akshaya college of Engineering and Technology, Kinathukadavu, Tamil Nadu, India

ABSTRACT

A personal health record is simply a collection of information about patient's health. If the patients have a shot record or a box of medical papers, they already have a basic personal health record. And they have probably encountered the big drawback of paper records. The hospital may rarely have their details with them. The Electronic personal health record systems remedy that problem by making patient's personal health record accessible to you anytime via a web enabled device, such as your computer, phone or tablet. Personal health records are not the same as electronic health records or electronic medical records, which are owned and operated by doctors' offices, hospitals or health insurance plans. There are a growing number of doctor's offices using these systems, but those that do often limit your access to and control of your medical record.

Keywords : Medical Data Access, web enabled device, Personal health record, AES, Electronic Healthcare, Electronic Medical Record Template

I. INTRODUCTION

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass

access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

1.1Configuring Organization and dataset.

This is the initial module of this project. Here the environment will be the medical domain. So this module contains a hospital environmental based application. An admin is available for controlling the whole application. Admin can create doctor, patient and actors those who can access this application. Admin can customize the whole application and provide rights and customization to the actors.

1.2 De Centralized the mining server

In order to access all the data, we need a centralized server. This server contains all the information about the organization like doctor details, patient details, patient's treatment information, treatment history, Medical reports, insurance details and etc. This de centralized server is for the entire hospitals county wide. Actors will be separated according to their roles and responsibilities. A unique code will be generated for all doctors and patients. So that fake doctors will be identified easily.

1.3. Dual Key Encryption

The de centralized server's data will be encrypted dual times before reaching the server. The entire data will be decrypted twice except the ID. The ID will represent the field for data access. Hybrid cryptography will be implementing for the encryption process. AES has a fixed block size of 128 bit and a key size of 128, 192, or 256 bit, has specified with block and key sizes in multiples of 32 bit, with a minimum of 128 bit. The block size has a maximum of 256 bit but the key size has no theoretical maximum AES operates on a 4×4 column-major order matrix of bytes, termed the state.

II. Related Works

2.1 SECURING PERSONAL HEALTH RECORDS IN CLOUD COMPUTING: PATIENT-CENTRIC AND FINE-GRAINED DATA ACCESS CONTROL IN MULTI-OWNER SETTINGS

Online PHR enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal health data. With the emergence of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, in order to enjoy the elastic resources and reduce the operational cost. However, by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers.

Under encryption, it is challenging to achieve fine-grained access control to PHR data in a scalable and efficient way. For each patient, the PHR data should be encrypted so that it is scalable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes.

Mostly designed for the single-owner scenarios. To reduce the key distribution complexity, the systems are dividing into multiple security domains, where each domain manages only a subset of the users. In this way, each patient has full control over her own privacy, and the key management complexity is reduced dramatically. Our proposed scheme is also flexible, in that it supports efficient and on-demand revocation of user access rights, and break-glass access under emergency scenarios.

Also, the patient should always retain the right to not only grant, but also revoke access privileges when they feel it is necessary. Therefore, in a "patient-centric" PHR system, there are multiple owners who encrypt according to their own ways, using different set of cryptographic keys. grained access control under encryption can be transformed into a key management issue. However, under the multi-owner setting, this problem becomes more challenging. Due to the large scale of users and owners in the PHR system, potentially heavy computational and management burden on the entities in the system can be incurred, which will limit the PHR data accessibility and system usability. On the one hand, for each owner her PHR data should be encrypted so that multiple users can access at the same time. But the authorized users may come from various avenues, including both persons who have connections with her and who do not.

2.2 SECURING THE E-HEALTH CLOUD

Modern information technology is increasingly used in healthcare with the goal to improve and enhance medical services and to reduce costs. In this context, the outsourcing of computation and storage resources to general it providers has become very appealing. E-health clouds offer new possibilities, such as easy and ubiquitous access to medical data, and opportunities for new business models. However, they also bear new risks and raise challenges with respect to security and privacy aspects. In this paper, point out several shortcomings of current e-health solutions and standards, particularly they do not address the client platform security, which is a crucial aspect for the overall security of e-health systems. To fill this gap, present security architecture for establishing privacy domains in e-health infrastructures. Our solution provides client platform security and appropriately combines this with network security concepts. Moreover, discuss further open problems and research challenges on security, privacy and usability of e-health cloud systems.

The application of information technology to healthcare has become increasingly important in many countries in the recent years. There are continuing efforts on national and international standardization for interoperability and data exchange. Many different application scenarios are envisaged in Electronic Healthcare (E-Health), e.g., electronic health records, accounting and billing, medical research, and trading intellectual property In particular e-health systems like Electronic Health Records (EHRs) are believed to decrease costs in healthcare (e.g., avoiding expensive double diagnoses, or repetitive drug administration) and to improve personal health management in general. Examples of national activities are the e-health approach in Austria, the German Electronic Health Card (EHC) system. Under development, or the Taiwan Electronic Medical Record Template (TMT).

In Germany each insured person will get a smartcard that not only contains administrative information (name, health insurance company), but also can be used to access and store medical data like electronic prescriptions, emergency information like blood group, medication history, and electronic health records. The smartcard contains cryptographic keys and functions to identify the patient and to encrypt sensitive data. The TMT in Taiwan concentrates on a standardized document data structure to ease information sharing, but also contains a similar infrastructure based on smartcards allowing to share and transfer EHRs. A common approach in all these systems is to store medical data in central data centers, which build the core concept of a centrally managed healthcare telemetric infrastructure. On the international basis the ISO (Technical Committee 215) and the Health Level 7 consortium (HL7) define standards for e-health infrastructures. While they also include specifications for security and privacy aspects, their main focus is currently the interoperability and definition of common document

exchange formats and nomenclature of medical data objects.

Obviously, e-health systems store and process very sensitive data and should have a proper security and privacy framework and mechanisms since the disclosure of health data may have s ever (social) consequences especially for patients. For example, banks or employers could refuse a loan or a job if the data about the health of a person is available. If health data is leaked outside the system deliberately or accidentally the responsible health professionals or its providers would have to face severe legal penalties for violating privacy laws.

2.3 ENERGY-EFFICIENT AND COVERAGE BASED DATA COLLECTION IN SPARSE WIRELESS SENSOR AND ACTOR NETWORKS

Wireless Sensor Networks (WSNs) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively transmit their data through the network to the destination point. Modern networks are bidirectional that includes controlling of sensor activity. In large WSNs, the events are relatively sparse compared to the number of sources. Also due deployment cost, the number of sensors is limited. In a sparsely connected network, a mobile actor can bridge the connectivity between groups of isolated nodes.

In such networks, sensors are mostly static and the mobile actors collect the data from these sensors. It then performs application dependent action. Such networks are termed as Wireless Sensor and Actor Networks (WSANs). The main characteristics of WSAN are the Sensor nodes are static and resource limited and the actors are usually resource-rich devices equipped with better processing capabilities, stronger transmission powers and longer battery life. Hence they can act on larger areas with high transmission power. For densely deployed sensors, actors are not needed as they have nodes to forward data to the destination the concept of a mobile actor is relatively new in the area of wireless sensor and actor networks. The main advantage of having a mobile actor is that more effective action can be taken, since the actor can get as close as possible to the event location. Additionally, in a densely connected network the presence of a mobile actor eases the problem of overburdened forwarding nodes by balancing the load among all the nodes in the network.

In a sparsely connected network, a mobile actor can bridge the connectivity between groups of isolated nodes. It is an overlay networks like peer to peer networks. WSAN is a hybrid network consisting of static sensor nodes which are sparsely distributed in the environment and actors, which are generally thought of being equipped with much more energy than sensors, move around to collect information from sensors and perform various networking or Application -dependent tasks.

In practice, the number of actors is much less than that of sensors due to budget limitation. Actors are sparsely distributed in the ROI. In this work, the problem of peer-to-peer networking for data dissemination among actors in WSANs is addressed, which consist of static sensors, responsible for environment monitoring, and mobile actors, in charge of data collection and task performing.

As sensors are energy constrained, efficiently disseminating data among actors and transmitting data to the base station with as less sensors involved as possible crucial to the overall network performance Recently, several WSN architectures based on Mobile Elements (MEs) have been proposed. Most of them exploit mobility to address the problem of data collection in WSNs. The main issues in

Energy-efficient peer-to-peer Message Dissemination (EMD) is that, the mobile elements will move randomly to collect data from the sensors, so it may lead to uncover some of the sensor in the particular regions. The sensors will store the message and forwarded to the other actors only when they come in contact. The energy of the sensors will drain out quickly due to data storage before it is forwarded.

2.4 DETECT THE PATH TO DELIVERY OF THE PACKET IN MOBILE ADHOC NETWORK

Cooperative networking is currently receiving significant attention as an emerging network design strategy for future mobile wireless networks. Successful cooperative networking can prompt the development of advanced wireless networks to cost-effectively provide services and applications in contexts such as Vehicular Ad Hoc Networks (VANETs) or mobile social networks. Two of the basic technologies that are considered as the core for these types of networks are Mobile Ad-Hoc Networks (MANETs) and opportunistic and Delay Tolerant Networks (DTNs).

The cooperation on these networks is usually contact based. Mobile nodes can directly communicate with each other if a contact occurs (that is, if they are within communication range). Supporting this cooperation is a cost intensive activity for mobile nodes. In the real world, nodes could have a selfish behavior, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources. The literature provides two main strategies to deal with selfish behavior: a) motivation or incentive-based approaches, and b) detection and exclusion.

The first approach, tries to motivate nodes to actively participate in the forwarding activities. These approaches are usually based on virtual currency and or game theory models. The detection and exclusion approach is a straight-forward way to cope with selfish nodes and several solutions have been presented. In CoCoWa, the author does not attempt to implement any strategy to exclude selfish nodes or to incentivize their participation and focus on the detection of selfish nodes.

2.5 MULTI-AUTHORITY ATTRIBUTE BASED ENCRYPTION IN CLOUD COMPUTING FOR AGRICULTURE

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a „cloud". It greatly attracts attention and interest from both academia and industry due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the best of our knowledge. First of all, data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control.

More likely, users want to control the privileges of data manipulation over other users or cloud servers. This is because when sensitive information or computation is outsourced to the cloud servers or another user, which is out of users" control in most cases, privacy risks would rise dramatically because the servers might illegally inspect users" data and access sensitive information, or other users might be able to infer sensitive information from the outsourced computation. Therefore, not only the access but also the operation should be controlled. Secondly, personal information (defined by each user's attributes set) is at risk because one's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life.

III. PROPOSED SYSTEM

In our proposed system, all the details that are currently maintained manually are computerized. Due to computerization, the data entered are very much secured, and cannot be accessed or changed by unscrupulous persons. The proposed system mainly helps to the all department.

2.1 FEATURES OF THE PROPOSED SYSTEM

- There should be entry screen and reports for all modules.
- The information's flow should be developed. Help messenger, alert, list of values
- Should be provided making the project user friendly.
- Database should be structured with minimum redundancy.
- System security should be provided

IV. METHODOLOGY

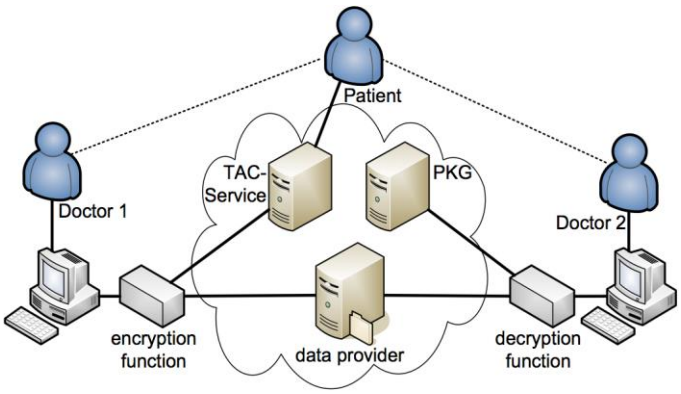
System testing is the state of implementation, which is aimed at ensuring that the system works accurately and efficiently as expect before live operation commences. It certifies that the whole set of programs hang together. System testing requires a test plan that consists of several key activities and steps for run program, string, system and user acceptance testing. The implementation of newly designed package is important in adopting a successful new system.

Testing is an important stage in software development. The system test in implementation stage in software development. The system test in implementation should be confirmation that all is correct and an opportunity to show the users that the system works as expected. It accounts the largest percentage of technical effort in the software development process.

3.1 TESTING

1. Knowing the specified function that a product has been designed to perform tests can be conducted to demonstrate each function is fully operational.
2. Knowing the internal workings of a product, tests can be conducted to ensure that "all gear mesh" that is, the internal operation of the product performs according to specification and all internal components have been adequately exercised.

3.2 Architecture



3.3 Implementation

Implementation is the stage in the project where the theoretical design is turned into a working system. The most crucial stage is achieving a successful new system & giving the user confidence in that the new system will work efficiently & effectively in the implementation state.

V. CONCLUSIONS

The system is similar to a decision support system that provides useful transformation to the decision makers of a college admin. This information helps in making decisions regarding assignment of frequently leave taking students and easily find out the leave particular along with the remaining leave. The system required by the client based on their input in a faster manner.

Since the Input given by the client is analyzed using the data mining techniques, an unknown or hidden information is retrieved from the data base.

VI. REFERENCES

[1]. Medinfo, Healthcare Information Management, http://elearning.hk.edu.tw/medinfo_4.pdf.

[2]. V. El-khoury, N. Bennani and A. M. Ouksel, "Distributed Key Management in Dynamic Outsourced Databases:

[3]. ATrie-Based Approach," 2009 First International Conference on Advances in Databases, Knowledge, and Data Applications, Gosier, 2009, pp.

[4]. Z. M. Ozsoyoglu and J. Wang, "A keying method for a nested relational database management system," [1992] Eighth International Conference on Data Engineering, Tempe, AZ, 1992, pp. 438-446.

[5]. Parthasarathi.P, Nivedha. S (Septemb2018), "Energy Efficient and Coverage based Data Collection in Sparse Wireless Sensor and Actor Networks" Published in International Journal of Computer Engineering and Applications, Volume 12, Special Issue, ISSN No:2321-3469.

[6]. Parthasarathi.P, Shankar. S (March 2017), "A Survival Study of Security Attacks, Mechanisms and Challenges in Network Security" Proceedings of Advanced in Natural and Applied Sciences (ANAS) ISSN NO: 1995 0772. (Anna University Annexure – II).

[7]. Parthasarathi.P, Shankar. S (March 2017), "Detect the path to Delivery of the Packet in Mobile ADHOC Network" Proceedings of Advanced in Natural and Applied Sciences (ANAS) ISSN NO: 19950772. (Anna University Annexure–II).

[8]. E. Bier man, T. Pretoria and E. Cloete, "Classification of Malicious Host Threats in Mobile Agent Computing" Proceedings of the 2002annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology, No. 5, pp. 34-49, 2002.

[9]. Kenneth. Loudon and Jane P. Laudon, Management Information Systems, Pearson, 07 March 2011, Chapter 6 Information systems Organizations and Strategy p.143.

Cite this article as :

Sh