ISSN: 0975-766X

CODEN: IJPTFI

Available Online through ***Research Article***

www.ijptonline.com

OPASS BASED SECURITY FOR THE CLOUD MANAGED MEDICAL RECORDS

Dr.S.Sivasubaramanian [1], K.SriPrasadh[2], S.Mageshkumar [3]

[2,3] Research Scholar, Bharath Institute of Higher Education and Research, Bharath University, Chennai, India

[1] Professor, Dhanalakshmi Engineering College, Chennai, India.

Received on: 15.10.2016 *Accepted on: 22.11.2016*

Abstract

A Personal Medical Record has multiple Security Domains (SD), multiple owners, multiple attribute authorities (AA), and multiple users. Each Personal Medical Record owner's client application generates its corresponding public/master keys. The secret keys are distributed by the Personal Medical Record service and using KP-ABE (Key Policy Attribute Based Encryption) the user secret key is generated that embeds to the access structure. This secure system is further enhanced by the use of additional secure layer, a user authentication protocol named OPass which leverages a user's cell phone and short message service to thwart password stealing and password reuse attacks. OPass only requires each participating website to possess a unique phone number, and a telecommunication service provider in registration and recovery phases. Through OPass, users only need to remember a long-term password for login on all websites.

Introduction

Personal Medical Record has emerged as a patient-centric model of medical information exchange. Many old people have the need of long-term medication, and often take several kinds of medicine at the same time. Almost every one of them knows the frustration of missing doses and the worry about potential interactions among the medicine. Hence the cloud computing is used to store the details. But the Personal Medical Records are sensitive, hence different encryption techniques are used to encrypt each attribute. Besides this high level encryption, another layer of secure authentication is provided by using Opass protocol that avoids different attacks such as domino, dictionary and phishing attacks and usage of malware. We consider a Personal Medical Record system where there are multiple Personal Medical Record owners and Personal Medical Record users. The owners refer to patients who have full control over their own Personal Medical Record data, i.e., they can create, manage and delete it. There is a central server belonging to the Personal Medical Record service provider that stores all the owners' Personal Medical Record. The users may come from various aspects;

for example, a friend, a caregiver or a researcher. Users access the Personal Medical Record documents through the server in order to read or write to someone's Personal Medical Record, and a user can simultaneously have access to multiple owners' data. A typical Personal Medical Record system uses standard data formats. For example, continuity-of-care (CCR) (based on XML data structure), which is widely used in representative Personal Medical Record systems including Indio, an open-source Personal Medical Record system adopted by Boston Children's Hospital. Due to the nature of XML, the Personal Medical Record files are logically organized by their categories in a hierarchical way.

Related Work

To assure the patients' control over their own Personal Medical Record, it is a promising method to encrypt the Personal Medical Record 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- rained, cryptographically enforced data access control.

To achieve fine-grained and scalable data access control for Personal Medical Record, we leverage attribute based encryption (ABE) techniques to encrypt each patient's Personal Medical Record file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the Personal Medical Record 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. Further, another step for secure authentication is used in the form of OPass protocol which leverages a user's cell phone and short message service to thwart password stealing and password reuse attacks.

Securing Personal Medical Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings

Online personal medical record (PMR) enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal medical data. With the emergence of cloud computing, it is attractive for the PMR service providers to shift their PMR applications and storage into the cloud. However, by storing PMRs in the cloud, the patients lose physical control to their personal medical data, which makes it necessary for each patient to encrypt the user's PMR data before uploading to the cloud servers. Under encryption, it is challenging to achieve fine-grained access control to PMR data in a scalable and efficient way. To enable fine-grained and scalable access control for PMRs, we leverage attribute based encryption (ABE) techniques to encrypt each patients' PMR data. To reduce the key distribution complexity, we divide the system into multiple security domains, where each domain manages only a subset of the users. In this way, each patient has full control over their 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.

Securing the E-Medical Cloud

E-medical clouds cover over 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. Here, we point out several shortcomings of current e-medical solutions and standards; particularly they do not address the client platform security, which is a crucial aspect for the overall security of e-medical systems. To fill this gap, we present security architecture for establishing privacy domains in e-medical infrastructures. Our solution provides client platform security and appropriately combines this with network security concepts. Moreover, we discuss further open problems and research challenges on security, privacy and usability of e-medical cloud systems.

Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records

We explore the challenge of preserving patients' privacy in electronic medical record systems. We argue that security in such systems should be enforced via encryption as well as access control. Furthermore, we argue for approaches that enable patients to generate and store encryption keys, so that the patients' privacy is protected should the host data center be compromised. The standard argument against such an approach is that encryption would interfere with the functionality of the system. However, we show that we can build an e-client system that allows patients both to share partial access rights with others, and to perform searches over their records. We formalize the requirements of a Patient Controlled Encryption scheme, and give several instantiations, based on existing cryptographic primitives and protocols, each achieving a different set of properties.

Authorized Private Keyword Search over Encrypted Personal Medical

Records in Cloud Computing To ensure Patients' control over their own privacy, data encryption has been proposed as a promising solution. However, key functionalities of a PMR service such as keyword searches by multiple users become especially challenging with PMRs stored in encrypted form. Basically, users' queries should be performed in a privacy preserving way that hides both the keywords in the queries and documents. More importantly, in order to prevent unnecessary exposure of patients' PHI from unlimited query capabilities, each user's query capability should be authorized and controlled in a fine-grained manner, which shall be achieved with a high level of system scalability. Existing works in searchable encryption are unable to meet the above requirements simultaneously. Here, we formulate and address the problem of authorized private keyword searches (APKS) on encrypted PMR in cloud computing environments. We first present a scalable and fine-grained authorization framework for searching on encrypted PMR, where users obtain query capabilities from localized trusted authorities according to their attributes, which is highly scalable with the user scale of the system. Then we propose two novel solutions for APKS based on a recent cryptographic primitive, hierarchical predicate encryption (HPE), one with enhanced efficiency and the other with enhanced query privacy. In addition to document privacy and query privacy, other salient features of our schemes include: efficiently support multi-dimensional, multiple keyword searches with simple range query, allow delegation and revocation of search capabilities. We implement our scheme on a modern workstation, and experimental results demonstrate its suitability for practical usage.

E. Purely Automated Attacks on Pass Points-Style Graphical Passwords

Here various methods for purely automated attacks against Pass Points-style graphical passwords are introduced and evaluated. For generating these attacks, a graph-based algorithm to efficiently create dictionaries based on heuristics such as click-order patterns (e.g., five points all along a line) is introduced. Some of the methods combine click-order heuristics with focus-of-attention scan-paths generated from a computational model of visual attention, yielding significantly better automated attacks than previous work. One resulting automated attack finds 7%–16% of passwords for two representative images using dictionaries of approximately entries. Relaxing click-order patterns substantially increased the attack efficacy albeit with larger dictionaries of approximately entries, allowing attacks that guessed 48%–54% of passwords.

These latter attacks are independent of focus-of-attention models, and are based on image-independent guessing patterns. Our results show that automated attacks, which are easier to arrange than human-seeded attacks and are more scalable to systems that use multiple images, require serious consideration when deploying basic Pass Points-style graphical passwords.

F. Password Management Strategies for Online Accounts

Given the widespread use of password authentication there is growing concern about identity theft. Here, how current systems support poor password practices is discussed and potential changes in website authentication systems and password managers are also presented.

Users visualized threats from human attackers, particularly viewing those close to them as the most motivated and able attackers; however, participants did not separate the human attackers from their potentially automated tools. They sometimes failed to realize that personalized passwords such as phone numbers can be cracked given a large enough dictionary and enough tries. Here potential changes in website authentication systems and password managers are also presented.

G. Comparing Passwords, Tokens, and Biometrics for User Authentication

For decades, the password has been the standard means for user authentication on computers. However, as users are required to remember more, longer, and changing passwords, it is evident that a more convenient and secure solution to user authentication is necessary. Here we examine passwords, security tokens, and biometrics—which is collectively called authenticators—and compares these authenticators and their combinations. Here the effectiveness of authenticators against several attacks and suitability for particular security specifications such as compromise detection and non repudiation is discussed. Examples of authenticator combinations and protocols are described to show tradeoffs and solutions that meet are chosen.

A Large Scale Study of Web Password Habits

Here the results of a large scale study of password use and password reuse habits are reported. The study involved half a million users over a three month period. A client component on users' machines recorded a variety of password strength, usage and frequency metrics.

This allows measuring or estimating such quantities as the average number of passwords and average number of accounts each user has, how many passwords he/she types per day, how often passwords are shared among sites, and how often they are forgotten. Extremely detailed data on password strength, the types and lengths of passwords chosen is obtained. The data is the first large scale study of its kind, and yields numerous other insights into the role the passwords play in users' online experience.

I. Pass pet: Convenient Password Management And Phishing Protection

Passpet is a tool that improves both the convenience and security of website logins

Registration

User authentication includes login, registration, communication, online through a combination of techniques. User-assigned site labels (pet names) help users securely identify sites in the face of determined attempts at impersonation (phishing). We propose new improvements to these techniques, discuss how they are integrated into a single tool, and compare Pass pet to other solutions for managing passwords and preventing phishing.

OAMR (Opass Authenticated Medical Records)

Overview

The user controlled medical records are encrypted in cloud and they are made to access using the android mobiles using the application. The security concerns are enhanced using Opass authentication.

Architecture of OAMR

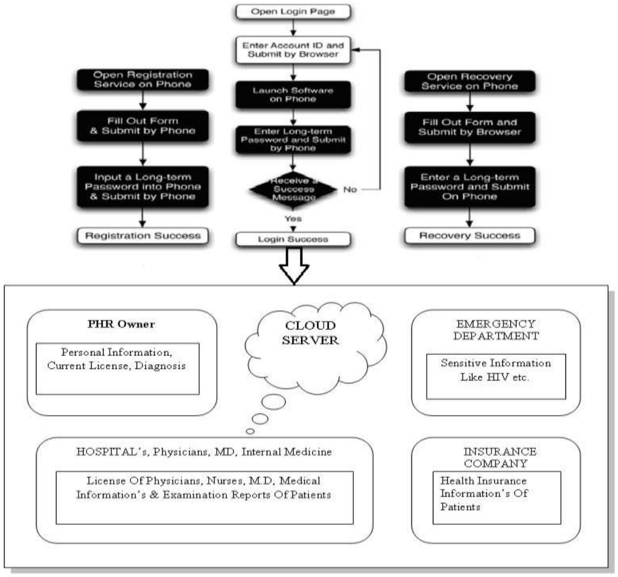
Open Login Page
Enter Account ID and Submit by Browser
Launch Software on Phone
Enter Long-term Password and Submit by Phone
Receive a Success Message
No
Yes
Login Success
Open Registration Service on Phone
Fill Out Form & Submit by Phone
Input a Long-term Password into Phone & Submit by Phone
Registration Success
Open Recovery Service on Phone
Fill Out Form and Submit by Browser
Enter a Long-term Password and Submit On Phone
Recovery Success
PHR Owner
Personal Information, Current License, Diagnosis
CLOUD SERVER
EMERGENCY DEPARTMENT
Sensitive Information Like HIV etc.
HOSPITAL's, Physicians, MD, Internal Medicine
License Of Physicians, Nurses, M.D, Medical Information's & Examination Reports Of Patients
INSURANCE COMPANY
Health Insurance Information's Of Patients

Fig: 1 Basic Framework of OAMR

payments and transaction. User details are handled in backend common database. Email validation and verification is needed to check whether the entered email id is valid and hence verified. The Long Term Password is generated based on the user details and it is stored in the database in encrypted format.

Login

The android application login process is done by identifying and authenticating the user details. The decryption process is done by Triple DES algorithm. The OTP is generated by using Triple DES algorithm. The OTP is entered into the web application for validation if true it goes to the application.

Recovery

Recovery phase is designated for some specific conditions; for example, a user may lose the cell-phone. The protocol is able to recover opass setting on the new cell-phone assuming that the user still uses the same phone number (apply a new SIM card with old phone number). Once user installs the opass program on the new cell-phone, he/she can launch the program to send a recovery request with the account ID and requested server ID to predefined TSP through a 3G connection. Similar to registration, TSP can trace the phone number based on the SIM card and forward the account ID to server through an SSL tunnel. Once the server receives the request, it probes the account information in its database to confirm if account is registered or not. If account ID exists, the information used to compute the secret credential will be fetched and be sent back to the user.

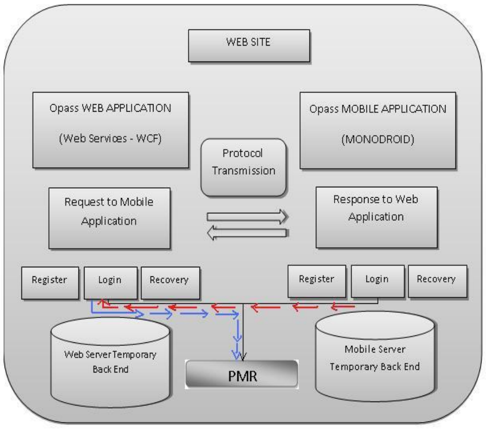

Fig: 2 Control Flow of OAMR.

Admin process

In admin process, the details such as patient's registration, Hospital registration, Insurance company registration and emergency hospital registration are stored in cloud space.

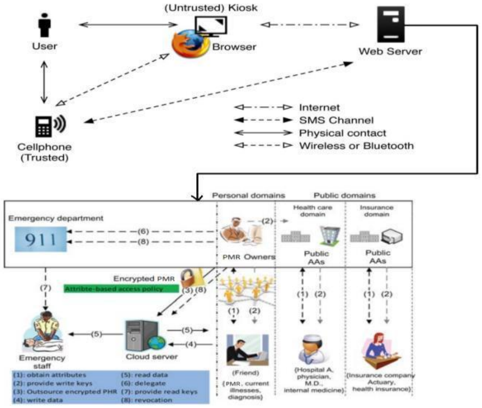

Fig: 3 Working of OAMR.

PMR Encryption and Access

The owners upload ABE-encrypted PMR files to the server. Each owner's PMR file is encrypted both under a certain fine- grained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the PMR files, excluding the server. For improving efficiency, the data attributes will include all the intermediate file types from a leaf node to the root. The data readers download PMR files from the server, and they can decrypt the files only if they have suitable attribute- based keys. The data contributors will be granted write access to someone's PMR, if they present proper write keys. User Revocation. Here we consider revocation of a data reader or their attributes/access privileges. There are several possible cases: 1) revocation of one or more role attributes of a public domain user; 2) revocation of a public domain user which is equivalent to revoking all of that user 's attributes. These operations are done by the AA that the user belongs to, where the actual computations can be delegated to the server to improve efficiency; 3). Revocation of a personal domain user's access privileges; 4) revocation of a personal domain user. These can be initiated through the PMR owner's client application in a similar way.

Policy Updates

A PMR owner can update the sharing policy for an existing PMR document by updating the attributes (or access policy) in the cipher text. The supported operations include add/delete/modify, which can be done by the server on behalf of the user.

Break-glass

When an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PMR. In our framework, each owner's PMR's access right is also delegated to an emergency department (ED). To prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify their identity and the emergency situation, and obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.

Conclusion

Implementing this novel framework will ensure secure sharing of personal medical records in cloud computing with OPass authentication scheme. In order to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their Personal Medical Records (PMR) to allow fine-grained access. The framework addresses the unique challenges brought by multiple Personal Medical Record owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize Attribute Based Encryption (ABE) to encrypt the PMR data, so that patient can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. Further-more, we enhance an existing Multi Authority Attribute Based Encryption (MA-ABE) scheme to handle efficient and on-demand user revocation, and prove its security. Besides this enhancement an additional enhancement is provided using an OPass authentication protocol which provides an additional layer of secure access to prevent password stealing and password reuse attacks simultaneously. Through implementation and simulation, we show our solution is both scalable and efficient.

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, in SecureComm'10 , Sept. 2010, pp. 89– 106.
2. H. L¨ohr, A.-R. Sadeghi, and MWinandy, ―Securing the e-health cloud,‖ in Proceedings of the 1st ACM International Medical Informatics Symposium , ser. IHI '10, 2010, pp. 220–229.
3. M. Li, S. Yu, N. Cao, and W. Lou, ―Authorized private keyword search over encrypted personal health records in cloud computing,‖ in ICDCS '11 , Jun.2011.
4. B. Ives, K. R. Walsh, and H. Schneider, ―The domino effect of password reuse, Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.
5. S. Gawand E. W. Felten, ―Password management strategies for online accounts,‖ in SOUPS '06: Proc. 2nd Symp. Usable Privacy. Security, New York, 2006, pp. 44– 55, ACM.
6. D. Florencio and C. Herley, ―A large-scale study of web password habits,‖ in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, 2007, pp. 657–666, ACM.
7. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, ―The design and analysis of graphical passwords,‖ in SSYM'99: Proc. 8th Conf. USENIX Security Symp., Berkeley, CA, 1999, pp. 1–1, USENIX Association.