DSAS A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System

ABSTRACT

In e-healthcare system, an increasing number of patients enjoy high-quality medical services by sharing encrypted personal healthcare records (PHRs) with doctors or medical research institutions. However, one of the important issues is that the encrypted PHRs prevent effective search of information, resulting in the decrease of data usage. Another issue is that medical treatment process requires the doctor to be online all the time, which may be unaffordable for all doctors (e.g., to be absent under certain circumstances). In this paper, we design a new secure and practical proxy searchable re-encryption scheme, allowing medical service providers to achieve remote PHRs monitoring and research safely and efficiently. Through our scheme DSAS, (1) patients' healthcare records collected by the devices are encrypted before uploading to the cloud server ensuring privacy and confidentiality of PHRs; (2) only authorized doctors or research institutions have access to the PHRs; (3) Alice (doctor-in-charge) is able to delegate medical research and utilization to Bob (doctor-in-agent) or certain research institution through the cloud server, supporting minimizing information exposure to the cloud server. We formalize the security definition and prove the security of our scheme. Finally, performance evaluation shows the efficiency of our scheme.

**EXISTING SYSTEM**

A reliable, searchable and privacy-preserving e-healthcare system was proposed by Yang *et al*. [45] based on searchable encryption [9], [18], [23], [40], [51] to protect sensitive healthcare files on cloud storage and enable cloud server to search on the encrypted data under the control of patients. The notion of public-key encryption with keyword search (PEKS) was proposed by Boneh *et al*. [8], who also gave the first PEKS construction for e-healthcare system in the public key environment. Later, Abdalla *et al*. [1] revisited the concept of PEKS and pro- posed the consistency notion. Baek *et al*. [3] extended PEKS which removes secure channels between a user and the cloud server, which make the patients communicate with doctors with a secure way. More expressive searchable schemes for e-healthcaer system are proposed in [24], [29], [33], and *zhang2017searchable*. To store a huge number of PHRs from multi users, schemes [24], [47] are proposed to optimize data storage and retrieval in the multi user setting.

Except for searchable encryption, proxy re-encryption (PRE) technology proposed by Blaze *et al*. [7] was also employed to store and share medical data in e-healthcare system. Proxy re-encryption is a highly promising solution for cloud computing, which has been widely applied to provide ciphertext transformation in cloud storage services recently. There has been significant progress in PRE over the recent years because of the property called *conditional transformation*, greatly enriching the commercial applications of PRE. In 2005, Ateniese *et al*. [2] pro- posed a unidirectional scheme and demonstrated how to prevent the proxy from colluding with delegatees in order text pose the delegator's private key. In 2006, Green and Ate-niese [17] extended the above notion to identity-based proxy re-encryption, and proposed a new CCA secure scheme.

Seo *et al*. [31] proposed the first proxy-invisible CPRE scheme that is secure against CCA secure in the standard model. He *et al*. [19] proposed a non-transferable proxy re-encryption scheme that solves the PKG despotism problem and key escrow problem. Fang *et al*. [12], [13] intro- duced fuzzy conditional proxy re-encryption and proposed a concrete construction based on the ``set overlap'' distance metric. In [20], PRE was deployed in mobile healthcare social network for a data owner to authorized a healthcare analyzer to access the owner's data. While the underlying purpose is similar, this proposal is more robust using CPRE and examines delegation of duty from a doctor to another, and further provides proxy-invisibility and condition-hiding properties.

Proxy re-encryption with keyword search (PRES), which is proposed by Shao *et al*. [32], can allow the patients to delegate his search and decrypt capability to doctor or research institution. In the e-healthcare system, suppose doctor Alice (del- egator) wants to delegate the search capability to doctor Bob (delegatee), by employing the PRES scheme propose by Shao *et al*. [32], 1) Bob can decrypt the ciphertexts delega ted from Alice using his own private key; 2) given a trapdoor from Bob, the mail gateway can test whether the ciphertext dele- gated from Alice contains some special keyword. However, we notice that with the re-encryption key, the proxy can transform all ciphertext of Alice no matter which keyword the ciphertext have. In this case, without Alice's delegation, Bob can still read all the message of Alice, this can be make serious security risks to the e-healthcare system. To address this issue, Weng *et al*. [38], [39] introduced the concept of conditional proxy re-encryption, where the re-encryption key is linked with a condition so that the delegatee can only decrypt ciphertext which satisfying the special condition. After that, a series of CPRE schemes have been proposed [12], [37], [41]. In most CPRE schemes, the condition is specified in the re-encryption key, and thus that the proxy can obtain the condition information such as ``HIV''. However, in the e-healthcare system, the condition can also contain some sensitive information [46]. Therefore, it is necessary to build a CPRE construction without leaking the condition information.

**Disadvantages**

* The system is not implemented a conditional proxy re-encryption searchable method to provide more security on datasets.
* The system is not implemented Hashing techniques on each datasets for more secure and safe data transaction.

Proposed System

In the proposed system,the following contributions have been developed

\_ *Uni-Directional*: Uni-directional proxy re-encryption is more superior than multi-directional proxy re encryption, otherwise, the delegatee may pass permissions to a third party, which will increase the disclosure of privacy. Hence, unidirectionality is a very important characteristic for e-healthcare system.

\_ *Proxy-Invisible*: In the secure e-healthcare system, if a malicious user can distinguish a re-encrypted ciphertext from an original ciphertext, it will increase the security risk such as the malicious user knows the delegator is

not available right now. Hence, e-healthcare system must provide proxy-invisible.

\_ *Condition-Hiding*: In the conditional proxy re-encryption scheme, the condition often contains some private information. If the condition is exposed, it will cause a great loss to the system. Obviously, if the proxy condition is hidden, the proxy server will get less sensitive information, which makes the e-healthcare system more secure.

\_ *Collusion-Resistance*: Inherent from trustworthy prop- erty, it is impossible to provide collusion-resistance when the dishonest proxy colludes with the delegatee

to export the delegator's private key, which would be a disaster to the e-heathcare system. As these authorized work are usually operated on the proxy server (assumed to be a third-party service provider), which for security reason is assumed to be untrusted. Hence, it is necessary to provide collusion-resistance in a secure e-healthcare system.

**Advantages**

1. Data privacy: patients' data collected by the sensor devices are encrypted before they are uploaded to the

cloud storage server. This ensures privacy and confidentiality of data since the cloud server will not be able to learn any information from the encrypted PHRs.

2. Conditional authorization: In the event where the doctor- in-charge (Alice) is unavailable, our scheme enables the delegation of the task to another doctor (Bob) through a cloud server, without the need to decrypt the PHRs thus minimizing information exposure to the cloud server.

3. Condition-hiding: Our scheme not only guarantees patients's PHRs privacy through encrypted data but also preserves the privacy of the condition embedded in the re-encryption key.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL