**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:**

* Yasnoff proposed a e-healthcare storage framework to eliminate the potential for loss of an entire centralized dataset from a single intrusion while maintaining reasonable search performance.
* A reliable, searchable and privacy-preserving e-healthcare system was proposed by Yang et al. based on searchable encryption to protect sensitive healthcare files on cloud storage and enable cloud server to search on the encrypted data under the control of patients.
* Boneh et al., gave the first PEKS construction for e-healthcare system in the public key environment. Later, Abdalla et al. revisited the concept of PEKS and proposed the consistency notion.
* Baek et al. extended PEKS which removes secure channels between a user and the cloud server, which make the patients communicate with doctors with a secure way.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Although encryption ensures data confidentiality and can be used to address concerns of data privacy and avoids the attacks from malicious users and cloud servers, it also brings inconvenience of usage. For instance, conventional encryption techniques render it difficult to query these encrypted data because of the useless information retrieval methods based on plaintext.
* The massive sensitive data leads to a great security and efficiency challenge to the current e-healthcare system due to lack of efficient information retrieve mechanism and poor fine-grained access control.
* Existing system also implies the doctors need to be available all the time. If the doctor is offline, then medical treatment would not be possible.
* Unfortunately, most existing CPRE schemes cannot guarantee the privacy of the condition, which also contains some sensitive information. On the other hand, if a malicious user can distinguish a re-encrypted ciphertext from an original ciphertext, it will increase the security risk such as that the malicious user knows Alice is not available right now.
* The existing system methods information retrieve over the encrypted PHRs is still a challenging issue, especially when dealing with massive data at a fine-grained level.
* Unfortunately, all the existing systems do not simultaneously support both encrypted keyword search and condition-hiding in practice, which limits the commercial applications of proxy re-encryption in the e-healthcare system.

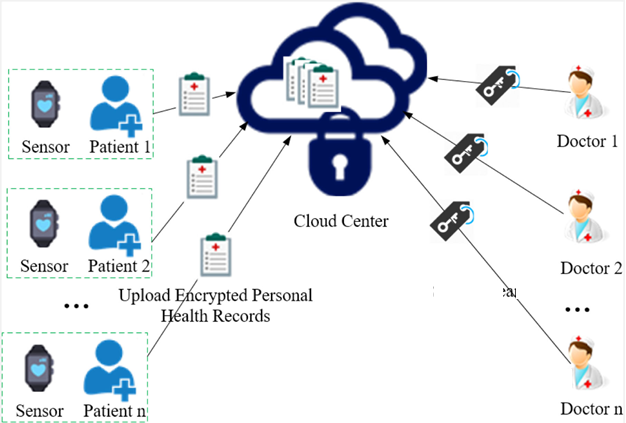
**PROPOSED SYSTEM:**

* We propose a proxy-invisible condition-hiding proxy re-encryption scheme with keyword search to address the issues of inefficiency and condition privacy in the e-healthcare system. Encrypting is considered to be a simple and efficient solution to guarantee data confidentiality, but it also makes search over encrypted data extremely difficult. Searchable encryption technology realizes the search operation of encrypted data without decryption, and solves the problem that users cannot control remotely because of data encryption. Hence, searchable is necessary in the e-healthcare system. In this proposed system, we aim to design an efficient, searchable and privacy-preserving e-healthcare system.
* In the proposed system we design a secure data sharing and authorized searchable scheme for e-healthcare system where patients continuously collects PHRs with sensors from physical environments and sends these encrypted PHRs to his doctor-in-charge for seeking for medical treatment. In some case, doctor A wants to share some but not all these PHRs to doctor B. To achieve access authorization, A generates a re-encryption key based on his private key and the public key of B. In order to prevent privacy disclosure, we generate a conditional re-encryption by embedding a trapdoor in the re-encryption key so that the cloud server can only convert ciphertext under the designated condition. Moreover, the cloud server is responsible for storing the encrypted data and providing keyword search services and also acts as a proxy to perform re-encryption for data users. When a keyword search request with a trapdoor is received from B, the cloud server performs information retrieval over the encrypted PHRs. Finally, B can decrypt ciphertext by using only his private key to obtain specific medical information.

**ADVANTAGES OF PROPOSED SYSTEM:**

* Data privacy: patients' data collected 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.
* 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.
* 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.
* Proxy invisibility: In our scheme, the authorized doctor (Bob) or a malicious user cannot distinguish which ciphertext is sent to delegatee and which ciphertext is re-encrypted by the cloud delegated by Alice.
* Collusion resistance: In our scheme, even a dishonest proxy colludes with Bob, Alice's private key can still be secure.

**SYSTEM ARCHITECTURE:**



**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium i3 Processor
* Hard Disk : 500 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 4 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 10.
* Coding Language : JAVA.
* Tool : Netbeans 8.2
* Database : MYSQL

**REFERENCE:**

LINLIN XUE, “DSAS: A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System”, IEEE Access (Volume: 10), 2022.