Unified Fine-grained Access Control for Personal Health Records in Cloud Computing

ABSTRACT

Attribute-based encryption has been a promising encryption technology to secure personal health records (PHRs) sharing in cloud computing. PHRs consist of the patient data often collected from various sources including hospitals and general practice centres. Different patients’ access policies have a common access sub policy. In this paper, we propose a novel attribute-based encryption scheme for fine-grained and flexible access control to PHRs data in cloud computing. The scheme generates shared information by the common access subpolicy which is based on different patients’ access policies. Then the scheme combines the encryption of PHRs from different patients. Therefore, both time consumption of encryption and decryption can be reduced. Medical staff require varying levels of access to PHRs. The proposed scheme can also support multi-privilege access control so that medical staff can access the required level of information while maximizing patient privacy. Through implementation and simulation, we demonstrate that the proposed scheme is efficient in terms of time. Moreover, We prove the security of the proposed scheme based on security of the ciphertext-policy attribute-based encryption scheme.

**EXISTING SYSTEM**

* Hohenberger et al. [25] proposed an online/offline technique to reduce the encryption complexity. The encryption of ABE was split into the plaintext-independent offline pre-computation and the plaintext-dependent online computation. The offline pre computation can produce intermediate ciphertext, which can be used with attributes to encrypt data online. However, this technique is only suitable for specific ABE schemes which have splittable algebraic structures.
* Rouselakis et al. [26], proposed two practical large-universe ABE schemes by expanding the system from unbounded hierarchical identity-based encryption (HIBE) [28] and ABE schemes in to prime order settings. The schemes are based on CP-ABE and KP-ABE, respectively, and have a significant improvement of the efficiency over [27]. However, the two schemes are both selectively secure. This means the security is guaranteed only for messages that are fixed before the adversary interacts with the system [29]. This is too restrictive for many realistic applications.
* Han et al. [30], proposed a privacy-preserving decentralized ABE scheme, where all the decryption keys of a user are tied to its global identifier (GID). Corrupted authorities cannot know the user’s attributes by tracing the GID from the decryption keys. Unfortunately, two users can pool their decryption keys to generate an unauthorized user’s decryption keys.
* **Disadvantages**
* The system doesn’t implemented Unified Access Control Framework which gives more security on Patient data.
* There is no Policy Based Access control for accessing patient’s data.

**PROPOSED SYSTEM**

* In this paper, we propose a new access control scheme for PHRs which can be provided by multiple patients. The scheme consists of ABE layer and symmetric key layer. In ABE layer, the scheme supports a multi-privilege access control for PHRs from multi-patients.
* The scheme combines the encryption of data from different patients where the data are under the same access policy to solve the problem of repetitive process in encryptions of these data, so that the cost of encryption and decryption can be reduced. The scheme achieves an efficient, flexible, and fine-grained access control on PHRs. In symmetric key layer, symmetric keys match medical workers’ access privileges and the keys with higher privilege can derive keys with lower privilege, not the other way around.
* The patients encrypt each class of data with corresponding symmetric keys in symmetric key layer, and encrypt the symmetric keys in the ABE layer. The system proves scheme is secure based on security of CP-ABE. We also conduct comprehensive experiments for the proposed scheme, and the simulation results demonstrate that the scheme has low computation complexity on encryption and decryption.

**Advantages**

* Data Confidentiality Preserving the confidentiality of PHR data is a key requirement for a PHR system.
* Collusion-resistance and Fine-grained and flexible access control on data.

**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