**THE CLOUD STORAGE AUDITING FRAMEWORK FOR DATA SHARING**

**ABSTRACT**:

Data sharing is one important service provided by cloud storage. In order to share data conveniently and securely, Shen et al. proposed a cloud storage auditing scheme for data sharing, which uses the sanitizable signature to hide sensitive information. However, it may cause unauthorized access to the data, since anyone can access the data stored on the cloud server. This article proposes a privacy-preserving cloud storage auditing (PP-CSA) scheme for data sharing, where only authorized users can access the data. Furthermore, PP-CSA adopts the Diffie–Hellman protocol to avoid the secure channel between the data owner and the sanitizer. Finally, the security analysis and the experimental results prove that the security and efficiency of PP-CSA can be accepted.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * In the scheme the medical doctor first blinds patient’s sensitive information in the EHR, and generates auditing authenticators for the blinded EHR. * Then, to unify the format of the blinded EHR and protect the hospital’s private information, the EHR information system administrator. * Meanwhile, the sanitizer transforms auditing authenticators without the medical doctor’s private key and makes the cloud storage auditing be performed effectively. | * We propose a PP-CSA scheme for data sharing, where only the authorized user can access the data. * We use the Diffie–Hellman protocol when the DO sends auditing authenticators to the sanitizer. And there is no need to establish a secure channel between the DO and the sanitizer in PP-CSA. * We give the security analysis, which proves that PP-CSA is a secure cloud storage auditing scheme with authorized access. Moreover, the experiment results show that PPCSA achieves desirable efficiency. |
| **EXISTING ALGORITHM**  third-party auditor(TPA) | **PROPOSED ALGORITHM:-**  privacy-preserving cloud storage auditing  (PP-CSA) |
| **ALGORITHM DEFINITION:-**  1)Auditing correctness: If the data stored in the CS is complete,  the generated proof can be verified by the TPA.  2) Authorization correctness: If the user’s authorization is  correct, the authorization can be verified by the CS. | **ALGORITHM DEFINITION:-**  A PP-CSA scheme for data sharing is mainly composed of the following six algorithms:   1. Setup (1k) 2. Key Gen (params , msk, ID) 3. Auth Gen (F, name, ID, sk) 4. Sanitization (F∗, θ∗) 5. Auditing (chal, F\_, θ, params) 6. Authorization (m, params): |
| **DRAWBACKS:-**   * sensitive information hiding * which uses a security out-sourcing algorithm to assist the DO to generate authenticators | **ADVANTAGES:-**   * the authorized user can access the file stored in the CS to protect the interests of the DO. * PP-CSA is secure and efficient. |

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS**:

System : Pentium i3 Processor

Hard Disk : 500 GB.

Monitor : 15’’ LED

Input Devices : Keyboard, Mouse

RAM : 2 GB

**SOFTWARE REQUIREMENTS:**

Operating system : Windows 10.

Coding Language : Java.

Tool : Netbeans 8.2

Database : MYSQL

**REFERENCE**:

Yan Xu , Long Ding, Jie Cui , Hong Zhong , and Jia Yu, “PP-CSA: A Privacy-Preserving Cloud Storage Auditing Scheme for Data Sharing”, IEEE SYSTEMS JOURNAL, 2021.