**Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage**

**Abstract:**

With cloud storage services ,users can remotely store their data to the cloud and realize the data sharing with others. Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud. In some common cloud storage systems such as the Electronic Health Records (EHRs) system, the cloud ﬁle might contain some sensitive information. The sensitive information should not be exposed to others when the cloud ﬁle is shared. Encrypting the whole shared ﬁle can realize the sensitive information hiding, but will make this shared ﬁle unable to be used by others. How to realize data sharing with sensitive information hiding in remote data integrity auditing still has not been explored up to now. In order to address this problem, we propose a remote data integrity auditing scheme that realizes data sharing with sensitive information hiding in this paper. In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the ﬁle and transforms these data blocks’ signatures into valid ones for the sanitized ﬁle. These signatures are used to verify the integrity of the sanitized ﬁle in the phase of integrity auditing. As a result, our scheme makes the ﬁle stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efﬁciently executed. Meanwhile, the proposed scheme is based on identity-based cryptography, which simpliﬁes the complicated certiﬁcate management. The security analysis and the performance evaluation show that the proposed scheme is secure and efﬁcient.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/UBUNTU.
* Implementation : NS2
* NS2 Version : 2.28
* Front End : OTCL (Object Oriented Tool Command  Language)
* Tool : Cygwin (To simulate in Windows OS)