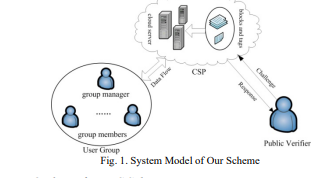
**PUBLIC INTEGRITY VERIFICATION OF SHARED GROUP DATA ON CLOUD STORAGE IS NOT POSSIBLE WITHOUT A CERTIFICATE**

**ABSTRACT**:

Cloud storage service supplies people with an efficient method to share data within a group. The cloud server is not trustworthy, so lots of remote data possession checking (RDPC) protocols are proposed and thought to be an effective way to ensure the data integrity. However, most of RDPC protocols are based on the mechanism of traditional public key infrastructure (PKI), which has obvious security flaw and bears big burden of certificate management. To avoid this shortcoming, identity-based cryptography (IBC) is often chosen to be the basis of RDPC. Unfortunately, IBC has an inherent drawback of key escrow. To solve these problems, we utilize the technique of certificateless signature to present a new RDPC protocol for checking the integrity of data shared among a group. In our scheme, user’s private key includes two parts: a partial key generated by the group manager and a secret value chosen by herself/himself. To ensure the right public keys are chosen during the data integrity checking, the public key of each user is associated with her unique identity, for example the name or telephone number. Thus, the certificate is not needed and the problem of key escrow is eliminated too. Meanwhile, the data integrity can still be audited by public verifier without downloading the whole data. In addition, our scheme also supports efficient user revocation from the group. The security of our scheme is reduced to the assumptions of computational Diffie-Hellman (CDH) and discrete logarithm (DL). Experiment results exhibit that the new protocol is very efficient and feasible.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * However, most of existing RDPC schemes are based on public key infrastructure (PKI). * Although PKI is widely used and occupies an important position in public key cryptography, there are still some security threats in it. For example, the security of PKI is based on the trustworthy of certificate authority (CA), but it is not an easy work to ensure the trustworthiness of CA | * The cloud server is not trustworthy, so lots of remote data possession checking (RDPC) protocols are proposed and thought to be an effective way to ensure the data integrity. * However, most of RDPC protocols are based on the mechanism of traditional public key infrastructure (PKI), which has obvious security flaw and bears big burden of certificate management |
| **EXISTING ALGORITHM**  identity-based cryptography (IBC) | **PROPOSED ALGORITHM:-**  RSA-based hash function was utilized to generate the authentication tag of the data) |
| **ALGORITHM DEFINITION:-**  Identity-based encryption (IBE), is an important primitive of [ID-based cryptography](https://en.wikipedia.org/wiki/ID-based_cryptography). As such it is a type of [public-key encryption](https://en.wikipedia.org/wiki/Public-key_encryption) in which the [public key](https://en.wikipedia.org/wiki/Public_key) of a user is some unique information about the identity of the user (e.g. a user's email address). This means that a sender who has access to the public parameters of the system can encrypt a message using e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user | **ALGORITHM DEFINITION:-**  Until now, lots of schemes [22-28] have been presented for the integrity verification of data shared in group. However, most of existing RDPC schemes [22-26, 28] are based on PKI. Although PKI is widely used and occupies an important position in public key cryptography, there are still some security threats in it. For example, the security of PKI is based on the trustworthy of certificate authority (CA), but it is not an easy work to ensure the trustworthiness of CA. |
| **DRAWBACKS:-**   * Less security * IBC has an inherent drawback of key escrow. * To solve these problems, we utilize the technique of certificateless | **ADVANTAGES:-**   * we prove the security of our scheme. * We implement our scheme and perform some experiments. * our scheme has good efficiency. |

**System Archuiture**

****

**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 : Eclipse

Database : MYSQL