**Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud**

**ABSTRACT**

More and more clients would like to store their data to public cloud servers (PCSs) along with the rapid development of cloud computing. New security problems have to be solved in order to help more clients process their data in public cloud. When the client is restricted to access PCS,  
he will delegate its proxy to process his data and upload them. On the other hand, remote data integrity checking is also an important security problem in public cloud storage. It makes the clients check whether their outsourced data are kept intact without downloading the whole data. From the security problems, we propose a novel proxy-oriented data uploading and remote data integrity checking model in identity-based public key cryptography: identity-based proxy-oriented data uploading and remote data integrity checking in public cloud (ID-PUIC). We give the formal definition, system model, and security model. Then, a concrete ID-PUIC protocol is designed using the bilinear pairings. The proposed ID-PUIC protocol is provably secure based on the hardness of computational Diffie–Hellman problem. Our ID-PUIC protocol is also efficient and flexible. Based on the original client’s authorization, the proposed ID-PUIC protocol can realize private remote data integrity checking, delegated remote data integrity checking, and public remote data integrity checking.

**EXISTING SYSTEM**

In public cloud environment, most clients upload their data to Public Cloud Server (PCS)and check their remote data’s integrity by Internet. When the client is an individual manager, some practical problems will happen. If the manager is suspected of being involved into the commercial fraud, he will be taken away by the police. During the period of investigation, the manager will be restricted to access the network in order to guard against collusion. But, the manager’s legal business will go on during the period of investigation. When a large of data is generated, who can help him process these data? If these data cannot be processed just in time, the manager will face the loss of economic interest. In order to prevent the case happening, the manager has to delegate the proxy to process its data, for example, his secretary. But, the manager will not hope others have the ability to perform the remote data integrity checking. Public checking will incur some danger of leaking the privacy. For example, the stored data volume can be detected by the malicious verifiers. When the uploaded data volume is confidential, private remote data integrity checking is necessary. Although the secretary has the ability to process and upload the data for the manager, he still cannot check the manager’s remote data integrity unless he is delegated by the manager. We call the secretary as the proxy of the manager. In PKI (public key infrastructure), remote data integrity checking protocol will perform the certificate management. When the manager delegates some entities to perform the remote data integrity checking, it will incur considerable overheads since the verifier will check the certificate when it checks the remote data integrity.

**Disadvantages of Existing System:**

1. In PKI, the considerable overheads come from the heavy certificate verification, certificates generation, delivery, revocation, renewals, *etc*.
2. In public cloud computing, the end devices may have low computation capacity, such as mobile phone, ipad, *etc*.

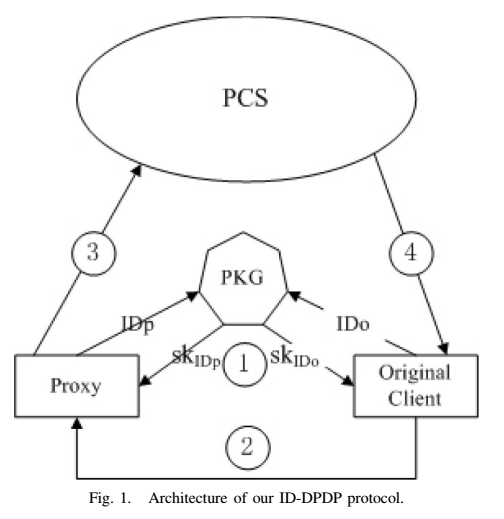
**PROPOSED SYSTEM**

In public cloud, this paper focuses on the identity-based proxy-oriented data uploading and remote data integrity checking. By using identity-based public key cryptology, our proposed ID-PUIC protocol is efficient since the certificate management is eliminated. ID-PUIC is a novel proxy-oriented data uploading and remote data integrity checking model in public cloud. We give the formal system model and security model for ID-PUIC protocol. Then, based on the bilinear pairings, we designed the first concrete ID-PUIC protocol. In the random oracle model, our designed ID-PUIC protocol is provably secure. Based on the original client’s authorization, our protocol can realize private checking, delegated checking and public checking.

**Advantages of Proposed System:**

1. The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis

**SYSTEM ARCHITECTURE**



**MODULES**

1. Original Client Module
2. Public Cloud Server Module
3. Proxy Module
4. Key Generation Center (KGC) Module

**Module Description:**

**Original Client:**

An entity, which has massive data to be uploaded to PCS by the delegated proxy, can perform the remote data integrity checking.

**PCS (Public Cloud Server):**

An entity, which is managed by cloud service provider, has significant storage space and computation resource to maintain the clients’ data.

**Proxy:**

An entity, which is authorized to process the Original Client’s data and upload them, is selected and authorized by Original Client. When Proxy satisfies the warrant mω which is signed and issued by Original Client, it can process and upload the original client’s data; otherwise, it cannot perform the procedure.

**KGC (Key Generation Center):**

An entity, when receiving an identity, it generates the private key which corresponds to the received identity.

**SYSTEM CONFIGURATION**

# Hardware Configuration

# Processor - Pentium –IV

* Speed - 1.1 Ghz
* RAM - 256 MB(min)
* Hard Disk - 20 GB
* Key Board - Standard Windows Keyboard
* Mouse - Two or Three Button Mouse
* Monitor - SVGA

# Software Configuration

* Operating System : Windows XP
* Programming Language : JAVA