ENABLING CLOUD STORAGE AUDITING WITH VERIFIABLE OUTSOURCING OF KEY UPDATES

ABSTRACT

Key-exposure resistance has always been an important issue for in-depth cyber defence in many security applications. Recently, how to deal with the key exposure problem in the settings of cloud storage auditing has been proposed and studied. To address the challenge, existing solutions all require the client to update his secret keys in every time period, which may inevitably bring in new local burdens to the client, especially

those with limited computation resources such as mobile phones. In this paper, we focus on how to make the key updates as transparent as possible for the client and propose a new paradigm called cloud storage auditing with verifiable outsourcing of key updates. In this paradigm, key updates can be safely outsourced to some authorized party, and thus the key-update burden on the client will be kept minimal. Specifically, we leverage the third party auditor (TPA) in many existing public auditing designs, let it play the role of authorized party in our case, and make it in charge of both the storage auditing and the secure key updates for key-exposure resistance. In our design, TPA only needs to hold an encrypted version of the client's secret key, while doing all these burdensome tasks on

behalf of the client. The client only needs to download the encrypted secret key from the TPA when uploading new files to cloud. Besides, our design also equips the client with

capability to further verify the validity of the encrypted secret keys provided by TPA. All these salient features are carefully designed to make the whole auditing procedure with key exposure resistance as transparent as possible for the client. We formalize the definition and the security model of this paradigm. The security proof and the performance simulation show that our detailed design instantiations are secure and efficient.

EXISTING YSTEM:

Our design is based on the structure of the protocol proposed. So we use the same binary tree structure as to evolve keys. This tree structure can make the protocol achieve fast key updates and short key size. One important difference between the proposed protocol and the protocol in is that the proposed protocol uses the binary tree to update the encrypted secret keys rather than the real secret keys. One problem we need to resolve is that the TPA should perform the outsourcing¬ computations for key updates under the condition that the TPA does not know the real secret key because it makes the key update difficult to be completed under the encrypted condition. Besides, it will be even more difficult to enable the client with the verification

capability¬ to ensure the validity of the encrypted secret keys. To address these challenges, we propose to explore the blinding technique with homomorphic property to efficiently "encrypt" the secret keys.

DISADVANTAGES OF EXISTING SYSTEM :

- In our scheme, the communicational messages comprise the challenge message and the proof message. we can see that the challenge message is linear with the number of checked blocks.
- The size of challenge message is 2.25 KB when the checked blocks are 100, and increases to 22.5 KB when the checked blocks are 1,000. As analyzed in [5], when the number of checked blocks is 460, the TPA can detect the data abnormity in the cloud with a probability at least 99%.
- In this case, the challenge message would be 10.35 KB. From we can see that the size of proof message varies with the depths of nodes corresponding to time periods. In period 0, the proof message is the shortest, which is 276.5 bytes, since the depth of the corresponding node is 0. And the longest proof messages appear at the leaves of the tree

PROPOSED SYSTEM:

We propose a new paradigm called cloud storage auditing with verifiable outsourcing of key updates. In this new paradigm, key-update operations are not performed by the client, but by an authorized party. The authorized party holds an encrypted secret key of the client for cloud storage auditing and updates it under the encrypted state in each time period. The client downloads the encrypted secret key from the authorized party and decrypts it only when he would like to upload new files to cloud. In addition, the client can verify the validity of the encrypted secret key.

We design the first cloud storage auditing protocol with verifiable outsourcing of key updates. In our design, the thirdparty auditor (TPA) plays the role of the authorized party who is in charge of key updates. In addition, similar to traditional public auditing protocols , another important task of the TPA is to check the integrity of the client's files stored in cloud.

ADVANTAGE OF PROPOSED SYSTEM:

- we propose to explore the blinding technique with homomorphic property to efficiently "encrypt" the secret keys. It allows key updates to be smoothly performed under the blinded version, and further makes verifying the validity of the encrypted secret keys possible.

- Our security analysis later on shows that such blinding technique with homomorphic property can sufficiently prevent adversaries from forging any authenticator of valid messages.
- Therefore, it helps to ensure our design goal that the key updates are as transparent as possible for the client. In the designed SysSetup algorithm, the TPA only holds an initial encrypted secret key and the client holds a decryption key which is used to decrypt the encrypted secret key.
- In the designed KeyUpdate algorithm, homomorphic property makes the secret key able to be updatedunder encrypted state and makes verifying the encrypted secret key possible.

SYSTEM SPECIFICATION

HARDWARE REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Sony.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS

- Operating system : Windows 7.
- Coding Language : ASP.Net with C#
- Data Base : SQL Server 2005.

- **8+ Years of Excellence in IEEE Project development for universities across INDIA, USA, UK, AUSTRALIA, SWEEDEN.**
- **Expert developers in JAVA , DOT NET , ANDROID , PHP, MATLAB , NS2 , NS3 , VLSI ,CLOUD SIM, TANNER , MICROWIND , EMBEDDED , ROBOTICS , MECHANICAL , MECHATRONICS , WIRELESS NETWORKS, OPNET , OMNET**
- **Over 11000+ projects , 425 clients - MICANS INFOTECH provides IEEE & application projects for CSE,IT,ECE,EEE,MECH,CIVIL,MCA,M.TECH,M.PHILL,MBA,DME,MS,PHD.**

Projects with FUTURE WORK / LIVE DEVELOPMENT / FACE TO FACE CLASSES

ONLY PROJECT CENTER WITH OWN DEVELOPERS - CSE, IT,ECE,MECH,CIVIL,EEE

PONDICHERRY – VILLUPURAM – CUDDALORE-CHENNAI