Data Security Using Lightweight Techniques in Mobile Cloud Computing

Engineering

KEYWORDS : Encryption based Scheme and Sharing based Scheme

Mrs Seema Hadke Department of Information Technology, BVCOEW, PUNE.

Nehal Jain Department of Information Technology, BVCOEW, PUNE.

Kanika Dhir Department of Information Technology, BVCOEW, PUNE.

Purva Kale Department of Information Technology, BVCOEW, PUNE.

Revati Karpe Department of Information Technology, BVCOEW, PUNE.

ABSTRACT

With the explosion of mobile applications and the support of Cloud Computing for a variety of services for mobile users, Mobile Cloud Computing (MCC) is introduced as an integration of cloud computing into the mobile environment. Mobile cloud computing brings new types of services and facilities for mobile users to take full advantages of cloud computing. It consists of front-end users who possess mobile devices and back end cloud servers. Here we have proposed two schemes for protecting the confidentiality and integrity of mobile data while uploading and downloading files to and from cloud respectively with backup facility of files. Here we have used two algorithms for the same. The Encryption based Scheme (EnS) tackles the situation where only one cloud server exists using AES technique for encryption. We proved that it guarantees the security goal and is the necessary condition for this situation. The Sharing based Scheme (ShS) allow a user to save data on multiple cloud also it further decrease the computation overhead by relying exclusive-or operations with cipher technique. All proposed schemes are resilient to the storage compromise on mobile devices, and all assume that the cloud servers are distrusted. Thus, they provide a stronger protection for more general and realistic application scenarios comparing with the previous work.

INTRODUCTION

Now a day a mobile device is becoming one of the important data processing devices for mobile users. A mobile device is still resource constrained and some applications generally need more resources than a mobile device can pay for. The resource limitations of mobile device confine users for executing intricate security operation using computational power of mobile device. To overcome this problem, a mobile device ought to get resources from an external source known as Cloud Computing platform. Mobile Cloud Computing refers to an infrastructure where storage and data processing can take place away from mobile device. Mobile device need not have a powerful CPU speed and large storage capacity. Keeping in mind the resource limitation of mobile device and need to ensure the confidentiality of the critical data, this paper, introduces the cryptographic version of Encryption based Scheme (EnS) and Sharing based Scheme (ShS) for secure data storage on Cloud with backup facility.

Existing System.

In Mobile Cloud Computing, Mobile Devices inherently need to migrate some computation and storage tasks to Cloud Servers. If Cloud servers are trusted, it would be perfect for the migration; but if CSs are distrusted, there will arise a critical problemi.e. how to maintain the outsourced computation and storage being trusted. In the existing system there is only one system for storage & retrieval of data to & from cloud, according to their efficiency.

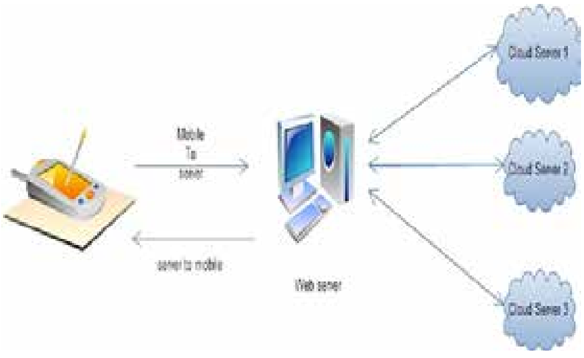

Figure 1: System Architecture

Proposed System

In this paper, we focus on the storage outsourcing in distrusted CSs (computation outsourcing is usually conducted in trusted CSs). After a MD creates a file and processes it, it may upload the file into a CS or multiple CSs. Host user or other cooperators may access it in the future in a distributed way. Obviously, the privacy and integrity of the file must be maintained in the storage of CSs during the period between uploading and accessing.

Proposed Schemes

In this section, we propose a family of schemes to solve the security requirement

Table 1 Notations

F	File (or Data) to be uploaded into Cloud side
FN	File Name of F
MA	Mobile Device
CS	Cloud Server
ENC(·,·)	Symmetric Key Encryption function
DEC(·,·)	Symmetric Key Decryption function
H(·)	Hash function
MAC	File Integrity Authentication Code
EnS	Encryption based Scheme
ShS	Sharing based Scheme

Encryption based Scheme (EnS)

In this scheme, file encryption and integrity checking are conducted by mobile device.The scheme EnS is described as follows:

Uploading process

(1) Before uploading file F into CS, MD prompts for asking U to input a password, denoted as PWD.
(2) MD generates encryption key EK= H(PWD || FN) and integrity key IK=H(FN || PWD) , where FN is the name of the file F (character string will be changed to bit string).
(3) MD encrypts F with EK as F′ = ENC(F,EK). MD generates file integrity authentication code, denoted as MAC = {H(F,IK)}.
(4) MD sends {F′ || H(FN) ||MAC} to portal CS. MD stores T = ⟨FN⟩ locally and deletes EK and IK.

Downloading process

(1) Suppose MD wants to fetch F with the name FN, MD then sends H(FN) to CS. CS searches in {F′,H(FN),MAC} sends back {F′ ||MAC} that matches H(FN) to MD.
(2) MD prompts for asking U to input corresponding PWD for the FN.
(3) MD generates encryption key EK= H(PWD || FN) and integrity key IK = H(FN || PWD).
(4) MD decrypts out F = DEC(F′,EK), and checks whether MAC = H(F, IK) is held.

As MD is semi-trusted (storage may be exposed but computation is usually properly conducted), PWD is not stored at MD. As PWD is memorable by U, the length is limited. To extend password entropy for defending brute force searching of PWD at CS, FN is included in the generation of EK and IK. FS is included for distinguishing each modification of file F with the same FN. EK and IK are distinct, for further improving the security. We state the analysis in detail in the following propositions.

Sharing based Scheme (ShS)

To further decrease the computation overhead, we propose a Sharing based Scheme. The scheme applies a simple XOR-based secret sharing method. That is, for sharing a secret s in n holders such that s can be recovered only when n holders are present, randomly generates n −1 shares and computes the last share by XORing n-1 with whole file.

Uploading process

(1) Before uploading file F into CS, MD prompts for asking U to input a password, denoted as PWD.
(2) Suppose d portal CSs are available. MD generates integrity key IK = H(FN || PWD).
(3) MD randomly generates d −1 files and computes last share by XORing d-1 share with whole file. Data is encoded using monoalphabetic cipher.MD generates MAC = {H(F, IK)} .
(4) MD sends {F′[j] || H(FN + j)}, 1<= j <= d to portal CS(j) , 1<= j <= d , in which a certain packet include MAC. MD stores T = {FN} locally and deletes IK.

Downloading process

(1) When MD wants to fetch F with the name FN, it sends H(FN + j) to CS(j) , where 1<= j<=d. CS(j) searches in its storage {F′[j] || H(FN + j)} according to H(FN + j) and sends back F′[j] to MD, in which a packet includes MAC.
(2) MD prompts for asking U to input corresponding PWD for the FN.
(3) Data is decoded and MD recovers F by XORing F′[i] from i=1 to d.
(4) MD generates integrity key IK=H(FN||PWD). MD checks whether MAC = H(F, IK) is held. Besides, the preparation stage for a cooperator is the same with that in the previous section. We thus propose

BACKUP OF SERVERS

The backup of the servers need to be taken in case fault occurs in any of the servers. So we implemented a backup scheme in which number of servers hold data of another server to save data from being corrupted or hacked. The scheme is represented in the below diagram. It can be explained as we have n number of servers, n backup files will be stored on the same servers. For e.g. Server A will have backup of Server C, Server B will have backup of Server A and Server C will have backup of Server B.

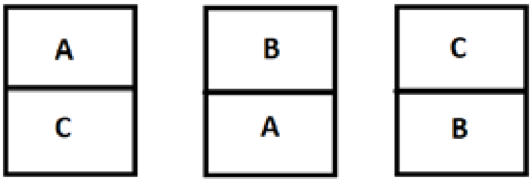

Figure 2: Backup of Servers

CONCLUSIONS

In this paper, we proposed a family of schemes for protecting the confidentiality and integrity of uploading files or data in mobile storage cloud. The scheme EnS tackles the situation where only one cloud server exists. We proved that it guarantees the security goal and is the necessary condition for this situation. The scheme ShS can further decrease the computation overhead by relying only on exclusive-or operations. The proposed schemes are resilient to the storage compromise on mobile devices, and all assume that the cloud servers are distrusted. Thus, they provide a stronger protection for more general and realistic application scenarios comparing with the previous work.

REFERENCE

[1] By Morten V. Pedersen, Member IEEE, and Frank H. P. Fitzek, Senior Member, "Mobile Clouds: The New Content Distribution Platform," Proceedings of the IEEE, Vol. 100, May 13th, 2012. | [2] Ki-Woong Park,Chulmin Kim and Kyu Ho Park, "BLAST:Applying Streaming Cipher into Outsourced Cloud Storage" in Computer Engg and Research Laboratory,2010. | [3] Monika Waghmare and Prof. T.A.Chavan, "Outsourcing with secure accessibility in Mobile Cloud Computing" in IJCTT, Volume 4, Issue 4, 2013. | [4] Karthik Kumar and Yung-Hsiang Lu, "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?" in Purdue University,Published by the IEEE Computer Society,2010. | |