USC Viterbi
School of Engineering

Multimedia Storage Security in Cloud Computing: An Overview

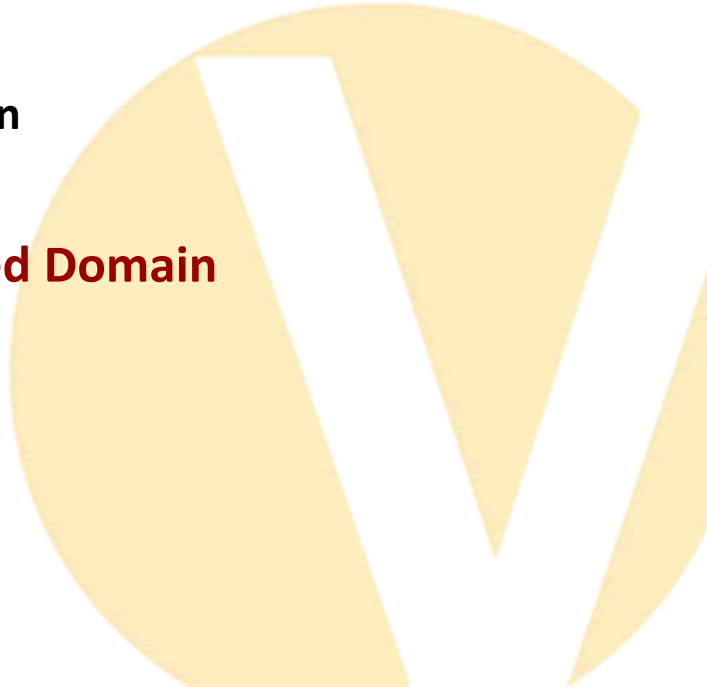
Chun-Ting Huang, Zhongyuan Qin and C.-C. Jay Kuo

USC

USC Viterbi School of Engineering

Outline

- Introduction
- Multimedia Storage and its Security
- Data Integrity
  - Proofs of Retrievability
  - Third Party Auditor
- Data Confidentiality
  - Fully homomorphic encryption
- Access Control
- Data Manipulation in Encrypted Domain
- Conclusion and Future Work



USC

USC Viterbi School of Engineering

Introduction

- **Rapid grow of needs for multimedia data transmission**
  - **Multimedia mails, orchestrated presentations, high-quality audio and video, collaborative multimedia documents**
- **Stored in cloud data storage server**
  - **Personal privacy issues**
  - **Security**

USC

USC Viterbi
School of Engineering

Security Service

- **Security services can be generally classified into five categories:**
  - **Data integrity**
  - **Authentication**
  - **Access control**
  - **Data confidentiality**
  - **Data integrity**
  - **Non-repudiation**

USC

USC Viterbi
School of Engineering

Storage Security Service

- **Based on category of security service, we classify papers of multimedia cloud storage security into:**
  - **Data integrity**
  - **Data confidentiality**
  - **Authentication**
  - **Access control**

USC

USC Viterbi School of Engineering

Overview of Multimedia Storage and Its Security

- **The architecture can be divided into five layers:**

Service Interface
Storage overlay
Metadata management
Storage management
Network and storage infrastructure

USC

USC Viterbi
School of Engineering

Cloud Computing Storage Security

- **There are many cloud computing service provider competing this market**
  - **Amazon, IBM, Google, Sun Microsystems, Microsoft, EMC, HP, Symantec, etc.**

- **Storage security**
  - **Physical storage security**
  - **Virtual data security**

USC

USC Viterbi
School of Engineering

Data Integrity

- **Trust mechanism between user and service provider**
  - **How to efficiently verifying the correctness of outsourced data stored in cloud server**
  - **Public will be reluctant to use the cloud storage service without the trust mechanism**

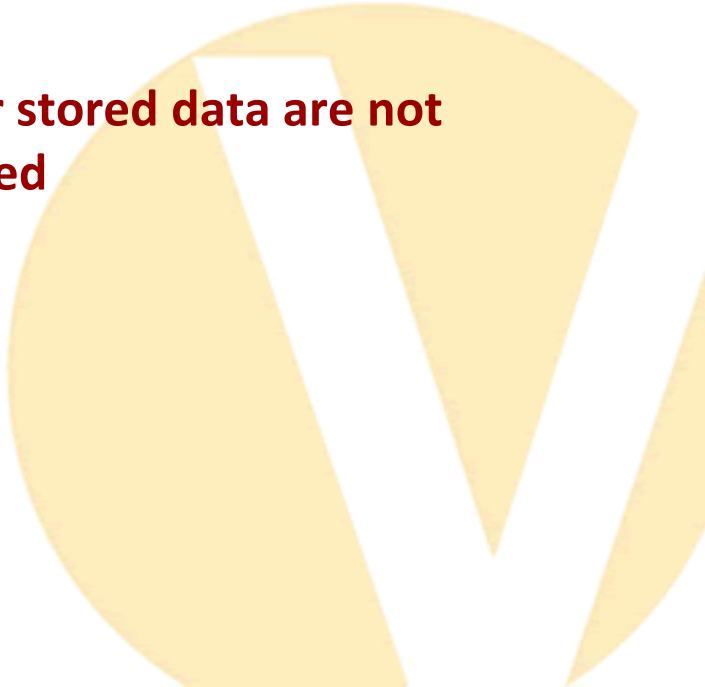
- **Proofs of Retrievability**
- **Third Party Auditor**

USC

USC Viterbi
School of Engineering

Proofs of Retrievability

- Proposed by Juels and Kaliski in 2007
- A system ensures the server (prover) to a client (verifier) that the stored data are intact during the storing and retrieving process of the client
- A guarantee to users that their stored data are not modified until they are retrieved



USC

USC Viterbi
School of Engineering

Ideal POR System Tasks

- **Efficient**
- **Publicly verifiable**
- **Publicly retrievable**
- **Unbounded use**
- **Stateless**

USC

USC Viterbi
School of Engineering

Process of POR

- POR protocol encrypts F and inserts randomly several *sentinels*
  - Each sentinels has the same outlook as other blocks
- To verify, user can ask prover for positions of a collection of sentinels
- Prover has to return the value at that position
- The comparison can show the stored data is deleted or modified if the returned value is different

USC

USC Viterbi School of Engineering

Other POR Scheme (1)

- **Provable Data Possession (PDP)**
  - **Proposed by Ateniese *et al.***
  - **Constructed based on symmetric key cryptography**
  - **Require no bulk encryption**

- **Combined model of Juels-Kaliski and Shacham-Waters**
  - **Proposed by Bowers *et al*.**
  - **Achieve lower storage overhead and tolerate higher error rates**

USC

USC Viterbi School of Engineering

Other POR Scheme (2)

- **Dynamic Data Support and Fairness**
  - **Proposed by Zheng and Xu**
  - **Fairness: prevents dishonest clients from accusing an honest server about modifying their stored data**
- **HAIL**
  - **Proposed by Bowers *et al*.**
  - **Integrity layer which extends the basic principle of RAID into Cloud**
  - **Remote checking mechanism provided security and efficiency**

USC

USC Viterbi School of Engineering

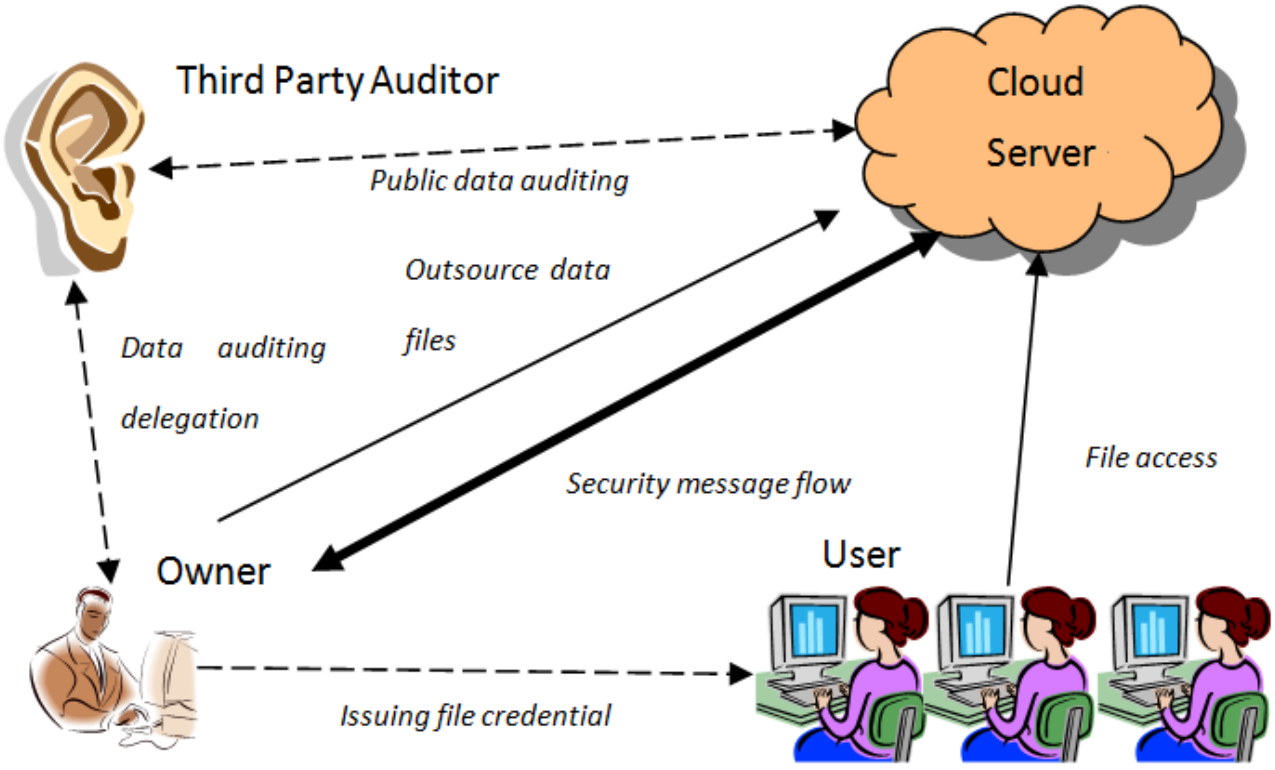
Third Party Auditor

- **A mechanism used to gain the trust on a service provider from its users**
  - ***Client*: which gives large data files to be stored in the cloud**
  - ***Cloud Storage Server (CSS)*: which is managed by Cloud Service Provider (CSP)**
  - ***Third Party Auditor (TPA)*: which can monitor and examine the stored file in cloud and is trusted to assess and expose risk of cloud storage services**

USC

USC Viterbi
School of Engineering

Third Party Auditor

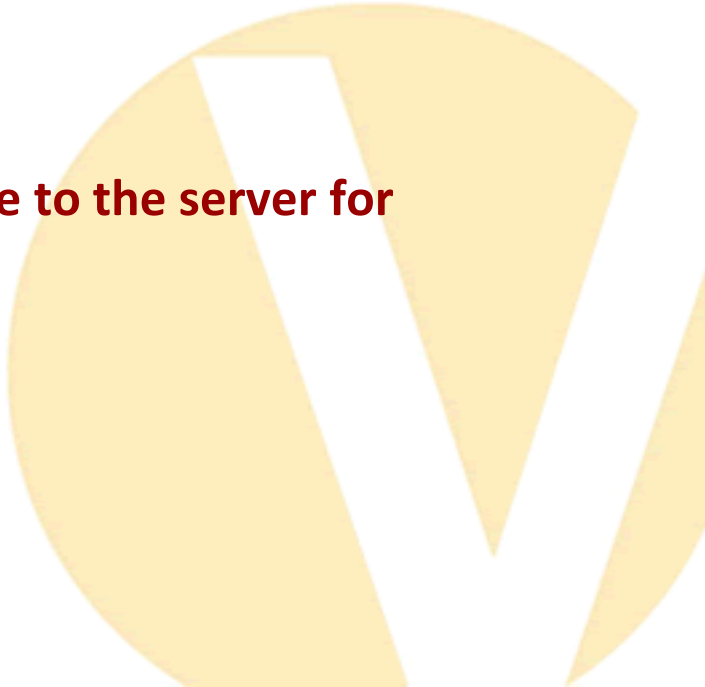


USC

USC Viterbi
School of Engineering

Process of TPA

- Public audit system allows a user to initialize his/her secret parameters of the system
- Send the verification metadata to TPA
- Audit the corresponding result
- TPA will issue an audit message to the server for checking user data



USC

USC Viterbi School of Engineering

Data Confidentiality

- **Cloud storage system should protect the data from unauthorized disclosure**
- **Fully Homomorphic encryption**
  - **Allows specific algebraic operations to be manipulated on a cipher text**
  - **Produces the same result as the same operation performs on the plaintext**

USC

USC Viterbi School of Engineering

Homomorphic Encryption

- **Partially homomorphic cryptosystem**
  - **Efficient and fast**
  - **Allows only one operation for the whole cryptosystem**
- **Fully homomorphic encryption (FHE)**
  - **Homomorphically evaluate circuits without knowing the input content**
  - **Practical solution for privacy-preserving model**

USC

USC Viterbi School of Engineering

First FHE (1)

- **Proposed by Craig Gentry**
- **Constructed by lattice-based cryptography**
  - **First stage: "*bootstrappable*" represented it can evaluate its own decryption circuit**
  - **Second stage: "*initial construction*" using lattices, which showed the basic model and the general flow of the scheme**
  - **Last stage: "*squash the decryption circuit*" technique for allowing circuit to be *bootstrappable***

USC

USC Viterbi
School of Engineering

First FHE (2)

- This scheme reduces the accumulated noise which caused by multiple algebraic operations
- Two security problems
  - worst-case scenarios over ideal lattices
  - sparse subset sum problem (SSSP)

USC

USC Viterbi School of Engineering

Second FHE

- **Homomorphic encryption over the integers**
  - **Proposed by Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan**
  - **a simplified version of the first FHE by using elementary modular arithmetic**
  - **somewhat homomorphic scheme over the integers**

USC

USC Viterbi School of Engineering

Access Control

- **Allow only data owners to access their data**
- **Various research approaches**
  - **Transfer customer's data location before uploading their data to the cloud storage server**
  - **Use different keys to encrypt each data block, flexible cryptographic access control can be realized**
  - **Separate content and format for handling and storing in different locations**
  - **Role-Based Access Control**

USC

USC Viterbi School of Engineering

Data Manipulation in Encrypted Domain

- **Data Search**
  - secure ranked keyword search in encrypted cloud data
  - Order-Preserving Symmetric Encryption
  - Search-as-a-service for the outsourced storage service
- **Data Recovery**
  - SCONEDB

USC

USC Viterbi
School of Engineering

Conclusion and Future Work

- This paper provides a brief overview on recently published papers and described some hot research topics in greater detail

- Multimedia cloud storage security is still in its infancy and expect to see more important breakthrough in the near future

USC