ECE 646, CRYPTOGRAPHY

PROJECT SPECIFICATION

GEORGE MASON UNIVERSITY

FALL, 2013

- Team members:
  - Kunal Pillai
  - Asrat Dea
  - Ravi Chandra Reddy Kambalapally

- **Cryptographic Security for Cloud Storage**
  - Cloud storage and security challenges
    - How does the cloud storage work?
    - Threat vulnerability of cloud storage system
  - Securing cloud data with encryption
    - Cryptographic protocols
    - Storing encrypted data
    - Downloading and decrypting data
    - Managing Access control of data
    - Securely sharing data in the cloud
    - Revocation of access key
- Introduction

Cloud storage technology is growing rapidly and gaining popularity in short time period. In recent years, when it comes to storing data, cloud storage is quickly becoming the method of choice. Accessibility, collaboration, scalability, and some other advantages that cloud storage provides are displacing traditional data storage to the cloud services. Data stored in the cloud can easily be accessed by using internet connection from anywhere regardless of users' location. These days, smartphones, tablets, and other mobile devices are wildly distributed and having connection to internet, and that has increased the interest of users to access their data storage from anywhere the move, which brings cloud storage to be good choice. In addition to accessibility, the cloud storage users can easily share their data in the cloud with anybody who has access to the storage.

These days people have all kinds of devices, for eg. an Iphone, Ipad, Mac. All of these have similar apps since they all have a similar operating system, the iOS. People want to keep the data between these devices in the same state so that all applications have the same kind of progress and everything can be shared between these devices. This leads to the use of cloud to synchronize data between devices.

Cloud storage also ends up being a reliable back if the security features are enforced. It is also resistant to hard drive crashes and the possibility of losing data is reduced tenfold.

These and other related benefits make cloud storage very attractive to the users..However, threat vulnerability and other security issues are highly discouraging the cloud storage users.

- Motivation

Fears over cloud security were not assuaged last year when Dropbox, a popular online cloud storage platform, was hacked yet again. This attack resulted in unauthorized access to employee accounts containing personal information of users, and spam being sent to users' personal folders. Despite the risks, most businesses are already using multiple cloud services to handle a myriad of business operations. The cloud is only going to become more important to us, and we must find ways to protect our data while getting the high quality performance we need. A large part of performance means adequate security.

Thus, looking into the existing security systems, evaluating them against sophisticated attacks, and looking for possible solutions are primary motives for this project.

Cloud security is very important and is still only in its nascent stages.Hence it is a topic that hasn't been explored as much. The research that is needed to secure the cloud has just begun. Hence we will analyze the current security implementations, understand all the nuances of the cryptographic techniques look into the possibilities of making stronger security for cloud storage.

❖ Hypotheses

Despite its flexibility and other benefits, security of cloud storage is issue of big concern. Security services such as confidentiality, availability, and data integrity are fundamental requirements a service provider should render. In this project we will perform an analytical assessment on deployment of cryptographic security on cloud storage. Cryptographic security mechanism is one of widely used security techniques and is claimed to be effective on the cloud. As cloud storage technology is new and rapidly growing with security risks, testing and deployment of cryptography is very crucial and this project analytically proceeds with the test

More precisely we will analyze if this service provides (at least):

- Confidentiality: the cloud storage provider does not learn any information about customer data
- Integrity: any unauthorized modification of customer data by the cloud storage provider can be detected by the customer while retaining the main benefits of a public storage service:
- Availability: customer data is accessible from any machine and at all times
- Reliability: customer data is reliably backed up

.

- Questions
  - What are cloud storage securities currently deployed?
  - What are the cryptographic protocols used in cloud security?
  - How is data stored in the cloud protected from an attack by a cloud service provider and its employees?
  - How does predicate encryption secure the cloud storage?
  - In what ways can a cloud service provider help with security?
  - How can a client help with security?

- Verification
  - Will subscribe to one of the cloud storage service vendors.
  - Encrypt, decrypt, and share data in cloud storage
  - Look for emulation techniques for cloud computing.
  - Once found, we can simulate a security feature on the cloud.
  - This will help us to verify our analysis of the current security features

- Goals to be achieved
  - Encrypting and securing data in motion and at rest
    - Subscribe to one of the cloud storage provider, encrypt data, and store it. While required to access the data download and decrypt it for usage.
  - Management of access control
    - Access control is very essential for preserving data security services. Access to the stored data will be given to particular people and access will be controlled. Unauthorized access to data will be inhibited and asses for assurance of security services.
  - Security implemented by provider
    - In addition to implementing cryptographic security for data storage, we would practice authentication and other security services the service provider deployed and analytically asses the reliability.
  - Security mechanisms implemented by clients
    - As cloud storage is highly gaining popularity, multiple people are subscribing to the service provider, and each of them may implement their own security mechanism for the provided that the system supports their mechanism. This project will analytically asses system supported client side security for the cloud storage.
  - Sharing data in cloud storage
    - One of the main advantages of cloud storage is sharing data among trusted groups. In this project we will practice sharing encrypted data among the group via reliable security mechanism.

❖ Possible change of specification

In plan-A, this analytical project will involve proxy devices to assist encryption/decryption process. However, based on situations, the plan may be changed to plan-B, which is using predicate encryption mechanism to carry out secured cloud storage. Predicate encryption process requires significant involvement in a cloud system with supporting technology. Depending on the services that renderthis technology we finally may pick up BoxCryptor application for encryption/decryption the data in cloud storage.

- Tentative table of contents
  - Table of contents
  - Abstract
  - Introduction
  - Background
  - Basic concepts of Cloud storage
  - Threat vulnerability of cloud storage
  - Cryptographic protocols used
  - Key exchange among data users
  - Encrypting and Decrypting data
  - Managing access control
  - Sharing data in cloud storage
  - Revoking access key
  - Findings and discussion
  - Summary and conclusions
  - Literature and references

References

[1] Reference books, Available:
William Stallings."Cryptography and Network Security"
Matt Bishop. "Computer Security"
Vic (J.R.) Winkler." Securing the Cloud"
http://www.amazon.com/Securing-Cloud-Computer-Security-Techniques/dp/1597495921
[2] "Predicate Encryption ", Available:
https://www.google.com/#q=predicate+encryption
[3] "Protecting Data in the Cloud ", Available:
http://web.mit.edu/newsoffice/2013/protecting-data-in-the-cloud-0702.html
[4] "Boxcryptor", Available:
https://www.boxcryptor.com/en/boxcryptor
[5] "Cryptography in the Cloud", Available:
http://www.bankinfosecurity.com/cryptography-in-cloud-a-3305/op-1
[6] "State of Cloud Encryption: From fiction to actionable reality", Available:
http://www.networkworld.com/news/tech/2013/040913-cloud-encryption-268542.html

[7] “A Distributed Access Control Architecture for Cloud Computing”, Available: http://www.infoq.com/articles/distributed-access-control-architecture-for-cloud-computing
[8] “Encryption Schemes of Access Control in Cloud Environments”, Available: http://ijns.femto.com.tw/contents/ijns-v15-n4/ijns-2013-v15-n4-p231-240.pdf
[9] “A Cryptographic Approach for Hierarchical Access Control in Cloud Computing”, Available: http://eprint.iacr.org/2013/208.pdf