Design and Implementation of Security System for Cloud Storage with AES Key Management

Min-Te Sun

Professor

Computer Science and Information Engineering

National Central University

Introduction

- Rising popularity of cloud computing
  - Development of computer technologies and the increasing computing power
- Cloud storage becomes an ideal way of storage for virtualized environment
  - Enterprises can focus on their service instead of computer infrastructure
  - High computing power, lower cost and better scalability
- Advantages of using cloud storage
  - Enterprises : lower cost and better management
  - Ordinary users: availability and efficiency

Motivation

- Concerns about security
  - The data owners may not have full control over their data in cloud
  - The cloud service provider can access users' personal data
- Data protection is the main challenge of cloud storage
  - For ordinary users, performance and efficiency of cloud storage are also big factors which will affect their inclination to migrate to the cloud

Related Work

- New frameworks or methods are developed to overcome the challenges of cloud storage
  - Security, efficiency, and load balancing
- Ensuring the security of users' data is the primary challenge in cloud storage
- Most proposed solutions can be categorized into cryptographic based and framework/protocol based

Ensuring Security via Cryptographic Techniques

- Bhandari et al.
  - A framework using RSA and HMAC techniques to enhance the data storage security
- Zhang et al.
  - A new encryption method using symmetric encryption and hardware encoding to improve security level of cloud storage
- Li et al.
  - A security structure of cloud storage based on the homomorphic encryption scheme

Ensuring Security via Cryptographic Techniques

- Arockiam and Monikandan
  - Encryption and obfuscation are used as two different techniques to protect the data in the cloud storage
- Azougaghe et al.
  - A simple, secure, and privacy-preserving architecture for inter-Cloud data sharing based on an encryption/decryption algorithm
- Concerns of these works
  - Causes additional computational load on client side
  - Requires additional hardware support

Ensuring Security via Framework or Protocol

- Shimbre and Deshpande
  - A framework using third party auditor and the AES algorithm. In the encryption procedure, the AES algorithm is used along with SHA-1
- Singh and Verma
  - A framework using AES, SHA-1, and Station-to-Station Key Agreement protocol to overcome security issues
- Feng et al.
  - A protocol with bidirectional verification for cloud storage security.

Ensuring Security via Framework or Protocol

- Yahya et al.
  - A security framework that protects data in cloud storage based on the level of protection it needs
- Feng et al.
  - A novel fair multi-party non-repudiation protocol, which provides a fair non-repudiation storage cloud and is capable of preventing roll-back attacks
- Concerns of these works
  - Focus on specific types of attack or network
  - Do not propose a proper encryption key management structure

Preliminary

- Advanced Encryption Standard
  - The formal encryption method adopted by the US Government.
  - A symmetric-key algorithm
    - Uses a single key as a part of the encryption process and decryption process
  - The key size of AES can be 128 bits, 192 bits, or 256 bits
  - A block cipher that uses an encryption key for several rounds of encryption.
    - Reads 8, 16 or 32 bytes from input data at a time and encrypts the data into block ciphers

Preliminary

- Secure Hash Algorithm
  - A special class of hash function for cryptography scenarios
  - A slight change of input will create significant change of result => The avalanche effect
  - A one-way function which cannot be reverted

Preliminary

- Password-Based Key Derivation Function
  - Part of RSA Laboratories' Public-Key Cryptography Standards (PKCS)
  - Makes keys much more difficult to break
  - Applies a pseudorandom function to a given password or passphrase along with a salt value to get a key

Problem Analysis

- Issues of Cloud Storage
  - User Verification
    - Cloud service provider (CSP) as the auditor
      - No supervision mechanism
  - Key Management
    - Encrypted files and their keys are stored in the same place
      - Vulnerable to attacks
      - CSP can get the origin content of encrypted files

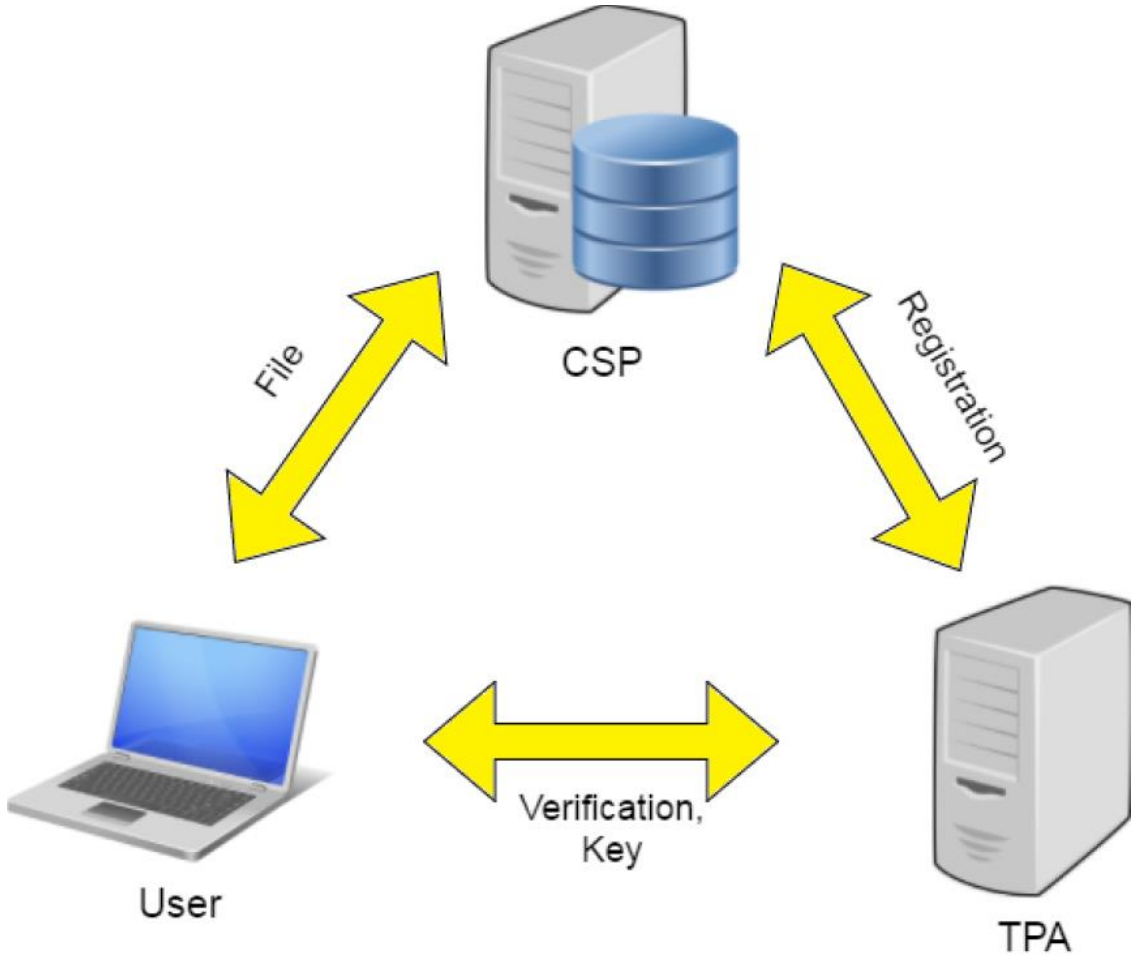
Problem Analysis

- Issues of Cloud Storage
  - Load-Balancing
    - Server carrying too much load
      - Server become the bottleneck of the system
      - Overall performance is limited by the computing power of the server
  - Performance of Encryption/Decryption
    - The balance between the security and performance
      - Security is the major concern of the users
      - Performance of the system is also a big factor for ordinary users

Design Goal

- Third party auditor for verification
- Proper key management and storage structure
- Low computational complexity
- Load-Balancing
- Efficient file encryption/decryption

System Model



System Model

- The user
  - Verified by TPA
  - Upload and download files to/from CSP
- The cloud service provider (CSP)
  - Offers the storage service to all users
  - Registration of users

System Model

- The third party auditor (TPA)
  - Verification of users' identity
  - Storing the keys of the encrypted files

Data Structure for Key Management

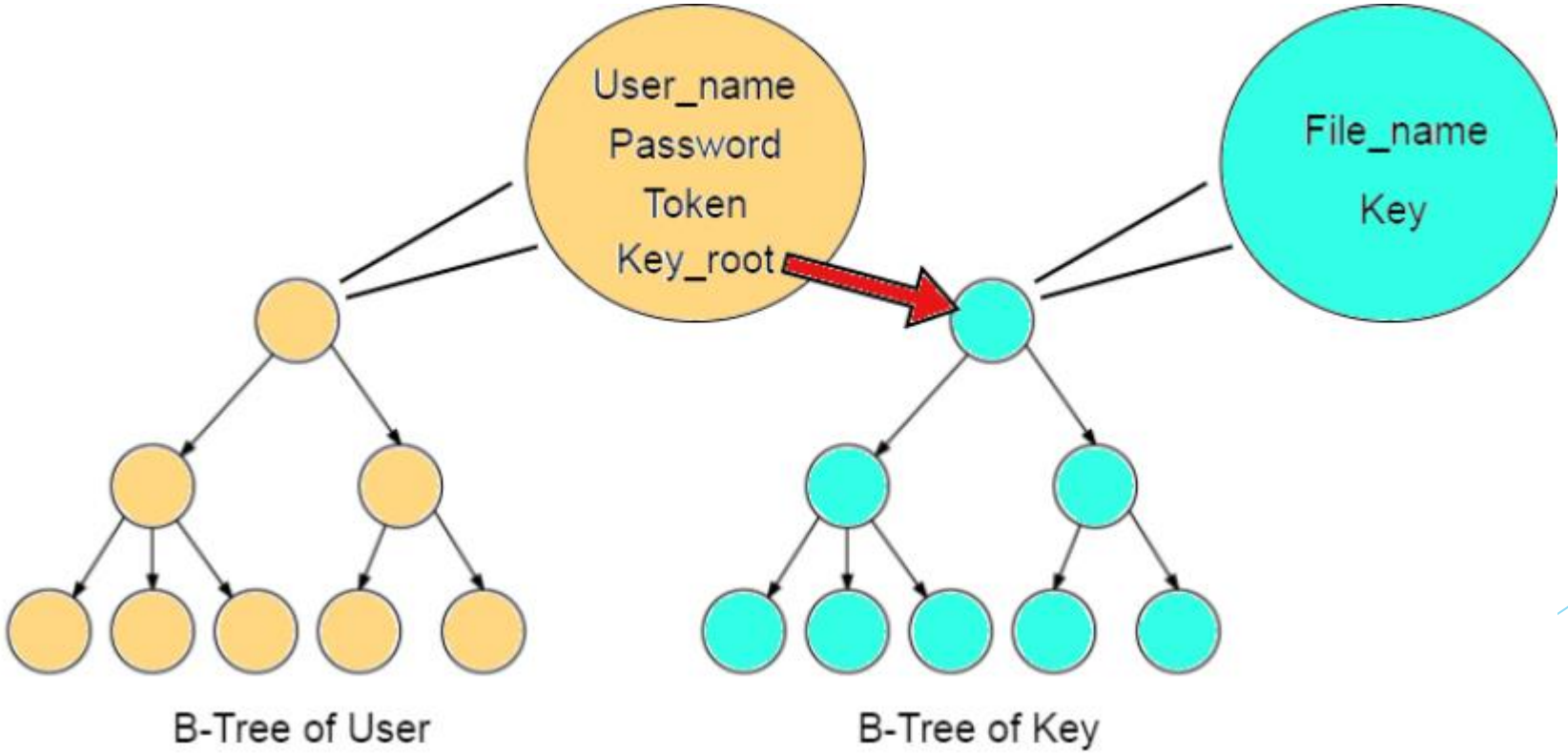
- Why?
  - The encrypted files and their keys are stored in different places
  - A lot of insertions and searches for keys
  - Handle the situation with minimum computational time and memory usage

Data Structure for Key Management

- B-tree
  - Optimized for systems which needs frequent searches and insertions of data.
  - The search, sequential access, insertion, and deletion of data can be done in logarithmic time

Data Structure for Key Management

- Data structure design for TPA



Data Structure for Key Management

- Implementation of user verification
  - B-tree of user account information
    - It will be used as soon as a user tries to get his identity verified
    - Has to be constructed before the authentication process at TPA server takes place

Data Structure for Key Management

- Implementation to find the encryption key for each user
  - B-tree of keys
    - Can be used to reduce the searching time
    - At the cost of the time building a B-tree(time complexity of

      O(n log n) with n nodes)
    - Static loading

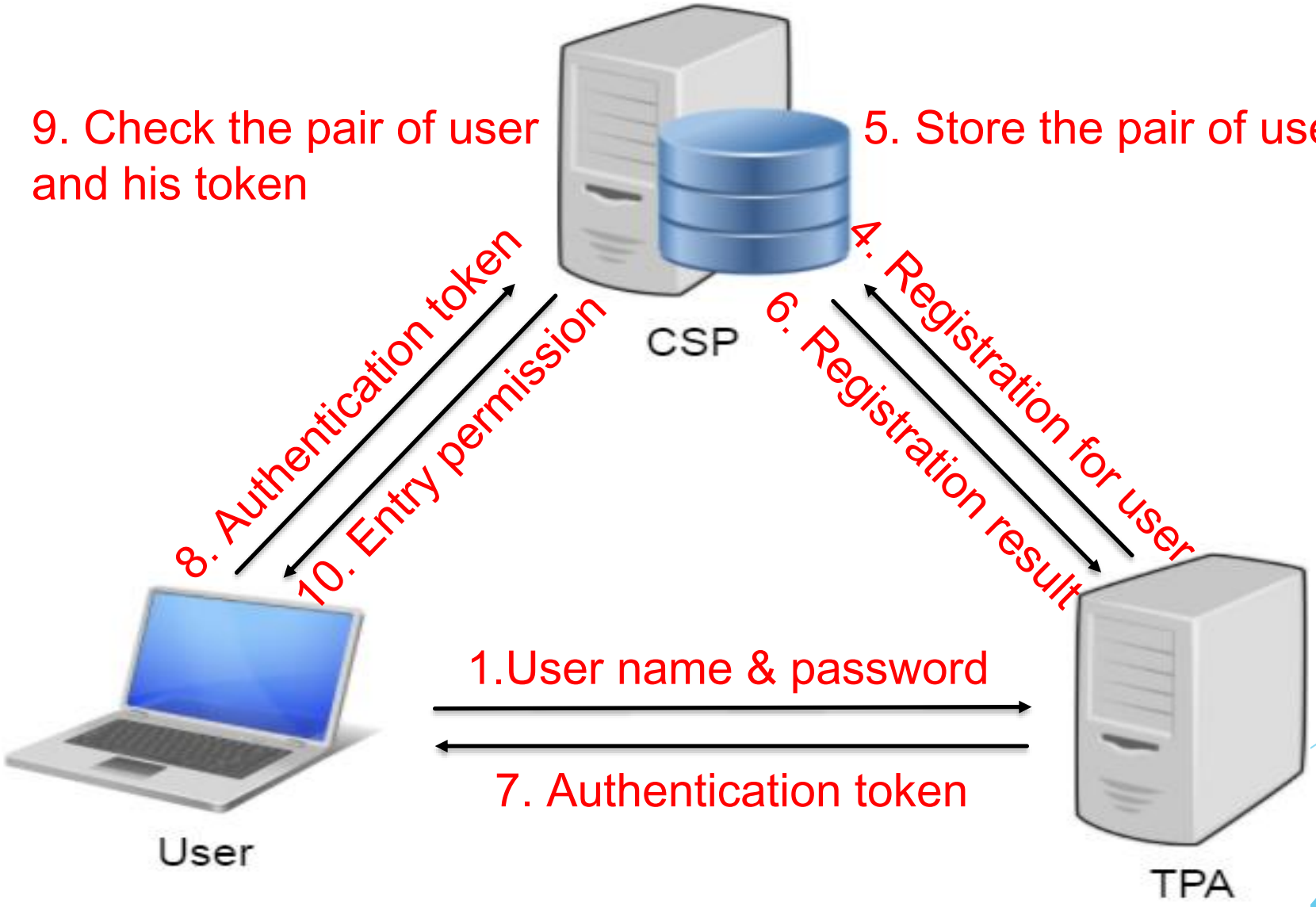
Data Structure for Key Management

- Implementation to find the encryption key for each user
  - Dynamic loading
    - Loads the specific key user requested from storage directly
    - Does not need to build to a B-tree
    - Requires to access the storage multiple times for different keys

Data Structure for Key Management

- Implementation to find the encryption key for each user
  - Speculation
    - If the users tend to access a large number of files
      - Static loading may perform better
    - If the users tend to access fewer files
      - Dynamic loading may perform better

Authentication Process



Authentication Process

- Authentication token
  - Only way to enter cloud storage system
  - One-time token
  - Prevent malicious users from trying to fake others' identity

Cryptographic Techniques and Key Management

- Building a system with load balancing
  - Each user has to carry some load
  - In our case, it is file encryption and decryption
  - Reduce the computational time on the user side is the first priority
  - Picking an efficient encryption algorithm is required

Cryptographic Techniques and Key Management

- Asymmetric encryption
  - Uses pairs of keys: public keys and private keys
  - Rarely used for file encryption nowadays due to its poor performance
  - Suffers from the limitation on the size of data it can handle
  - Extra expenses of key management

Cryptographic Techniques and Key Management

- Symmetric encryption
  - Utilizes the same key for encryption and decryption
  - Does not need complicated mathematical operations and is relatively easy and fast
  - Commonly used for file encryption due to its performance

Cryptographic Techniques and Key Management

- Advanced Encryption Standard (AES)
  - Performance
  - Security
    - Hard to break with a proper key
    - Around 10^{77} key combinations for AES-256
    - Takes around 9.36×10^{52} years to break for 33.86 petaflop supercomputer

Cryptographic Techniques and Key Management

- Issues of AES
  - The strength of the key
  - Sharing the key with other party
    - The safety of the transmission of keys to other party
    - The safety of the key management
  - In this research, we assume that the key is safe during transmission and focus on the key management and the strength of the key

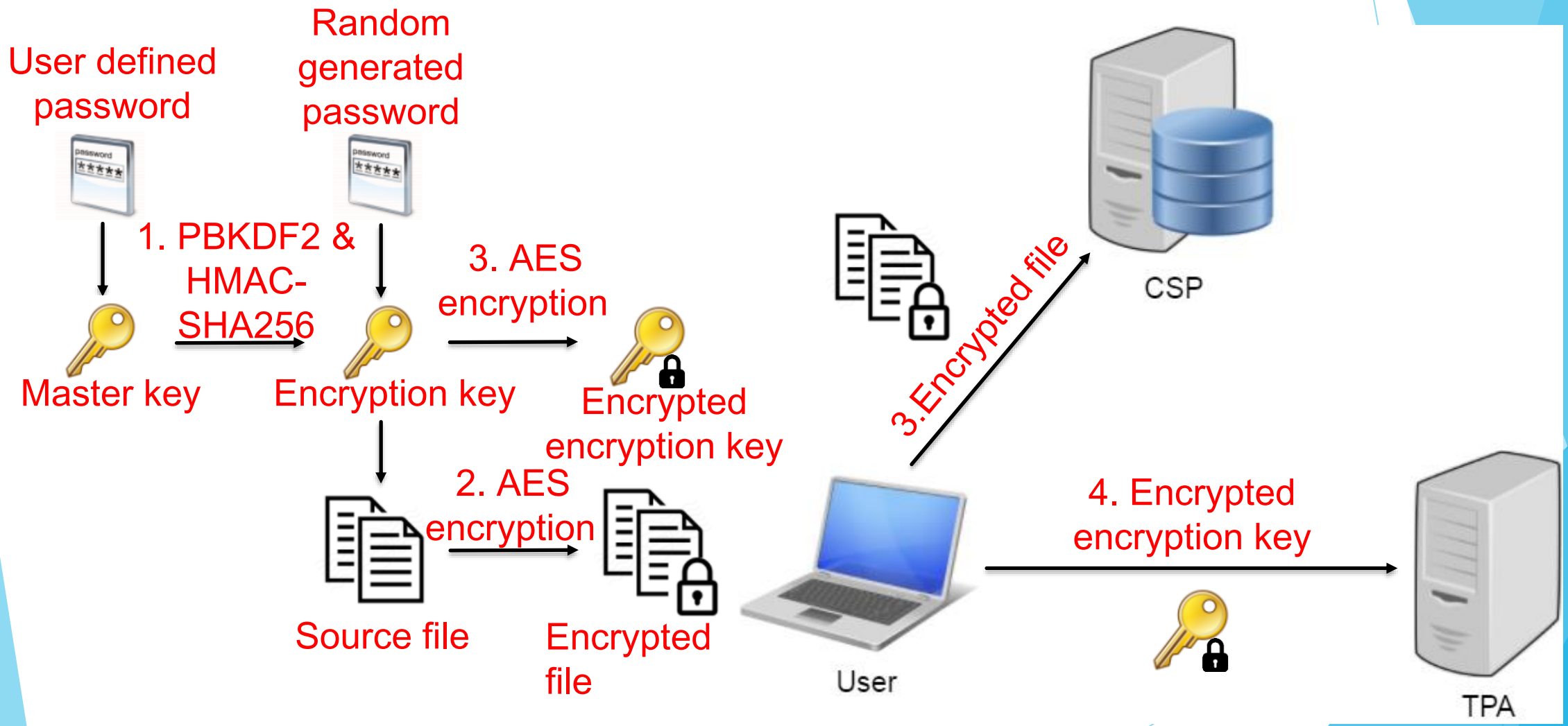
Cryptographic Techniques and Key Management

- Issues of AES
  - Ensure the strength of the key
    - Using Password-Based Key Derivation Function 2 (PBKDF2) and HMAC-SHA256 to generate encryption keys
    - In each round of PBKDF2, HMAC-SHA256 is applied along with a salt value. This process is repeated multiple rounds
    - Able to derive a strong key from a password

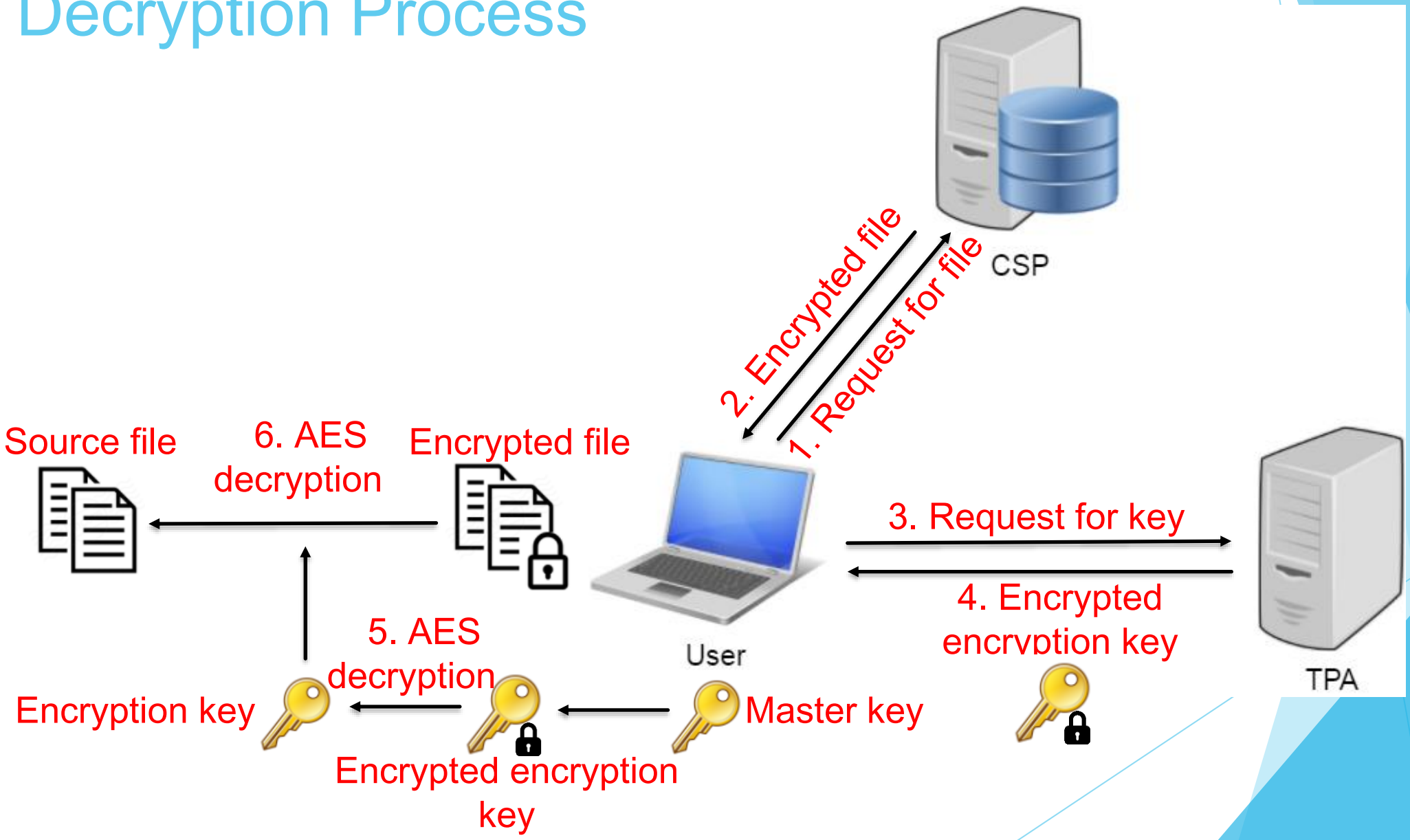
Cryptographic Techniques and Key Management

- Issues of AES
  - Ensure the safety of the key management
    - CSP or unauthenticated users cannot access encryption keys
    - What about TPA?
    - Master key for each data owner

Encryption Process



Decryption Process



Cryptographic Techniques and Key Management

- Our key management can be summarized as follows
  - Strength of key
  - Safety of key storage
  - Efficiency of key storage

Performance and Evaluation - Qualitative Analysis

- Security Analysis

Functions	Bhandari	Shimbre	Our Model
Identification	YES	YES	YES
Third party auditor	YES	YES	YES
Double authentication	YES	NO	YES
File encryption	YES	YES	YES
Strong key generation	NO	NO	YES
Key management	NO	NO	YES
Encrypted file protection	NO	NO	YES

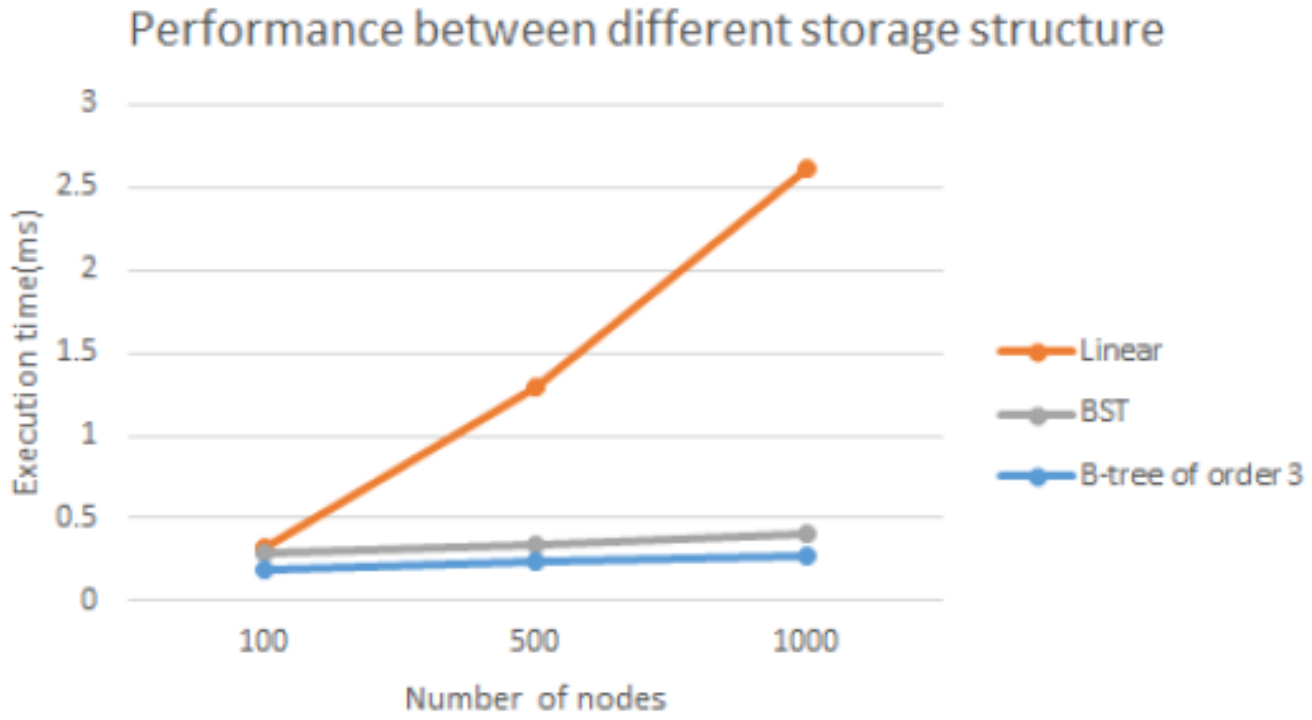
Performance and Evaluation - Quantitative Analysis

- The same configuration of personal computers (PCs) are used for both server and client

- The configuration of the PC is provided as follows.
  - Windows 10 64-bit
  - Intel Core i7-6700 CPU 3.40GHz
  - 16.0 GB RAM
  - Average 500Mbps/75Mbps download/upload speed measured by NTU network speed test

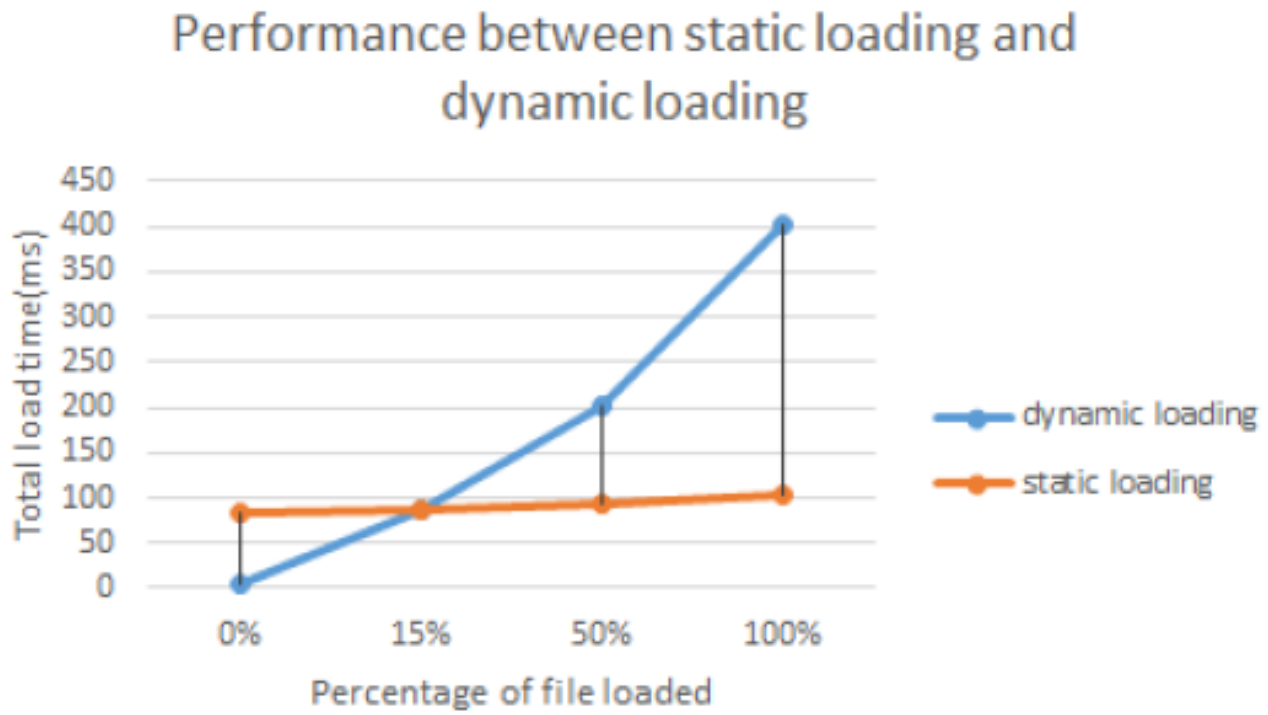
Performance and Evaluation - Quantitative Analysis

- Performance of Searching



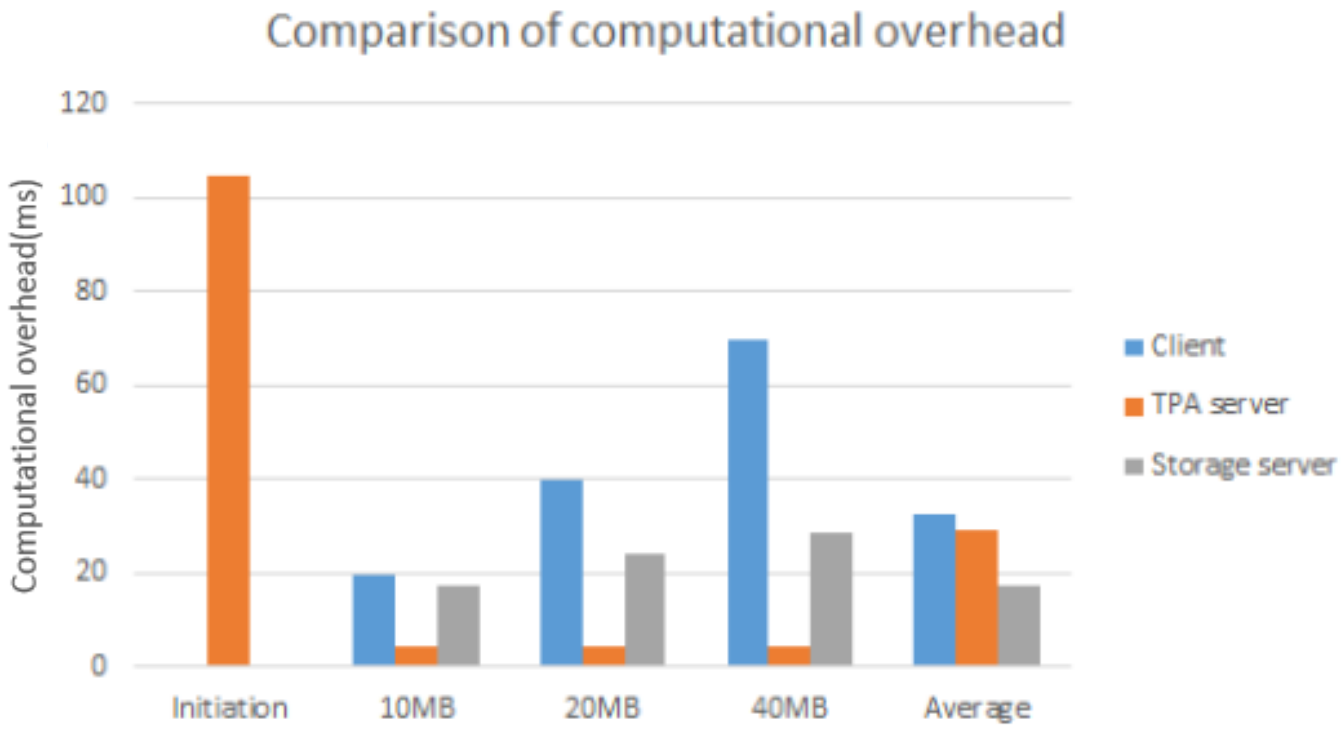
Performance and Evaluation - Quantitative Analysis

- Computational Load



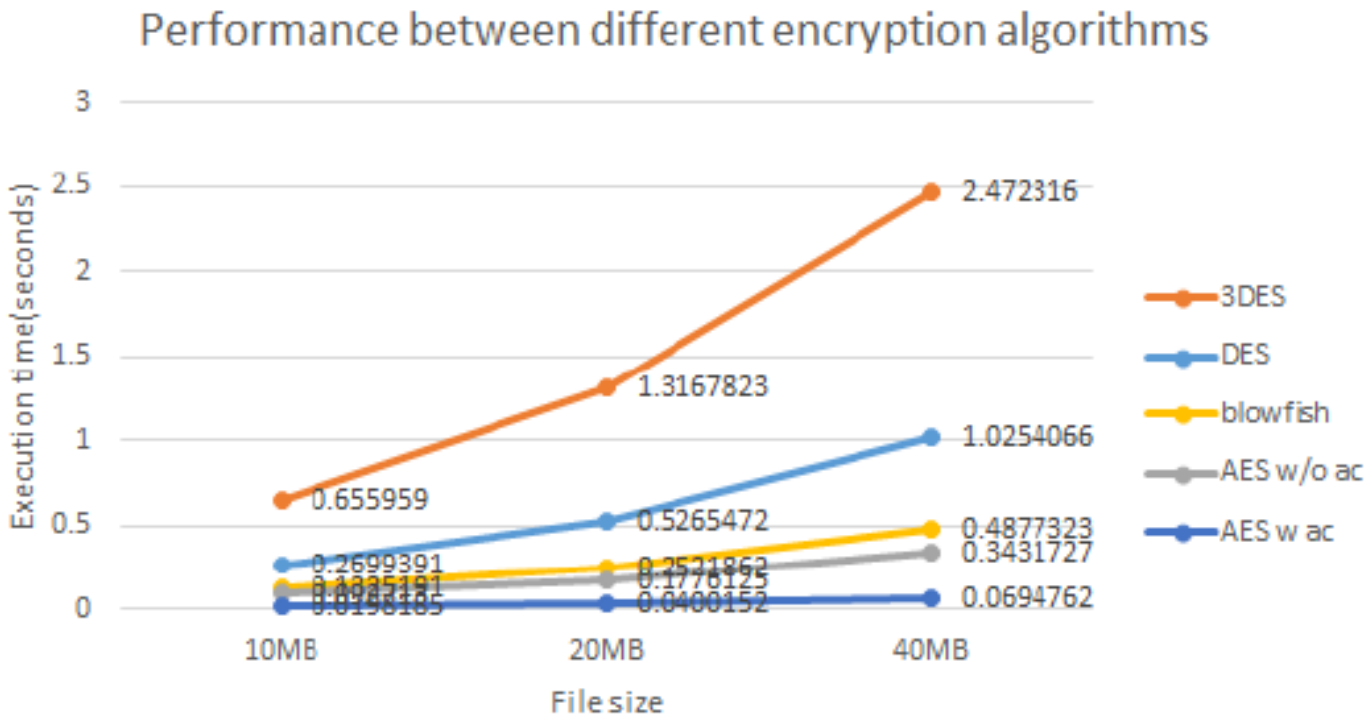
Performance and Evaluation - Quantitative Analysis

- Computational Load



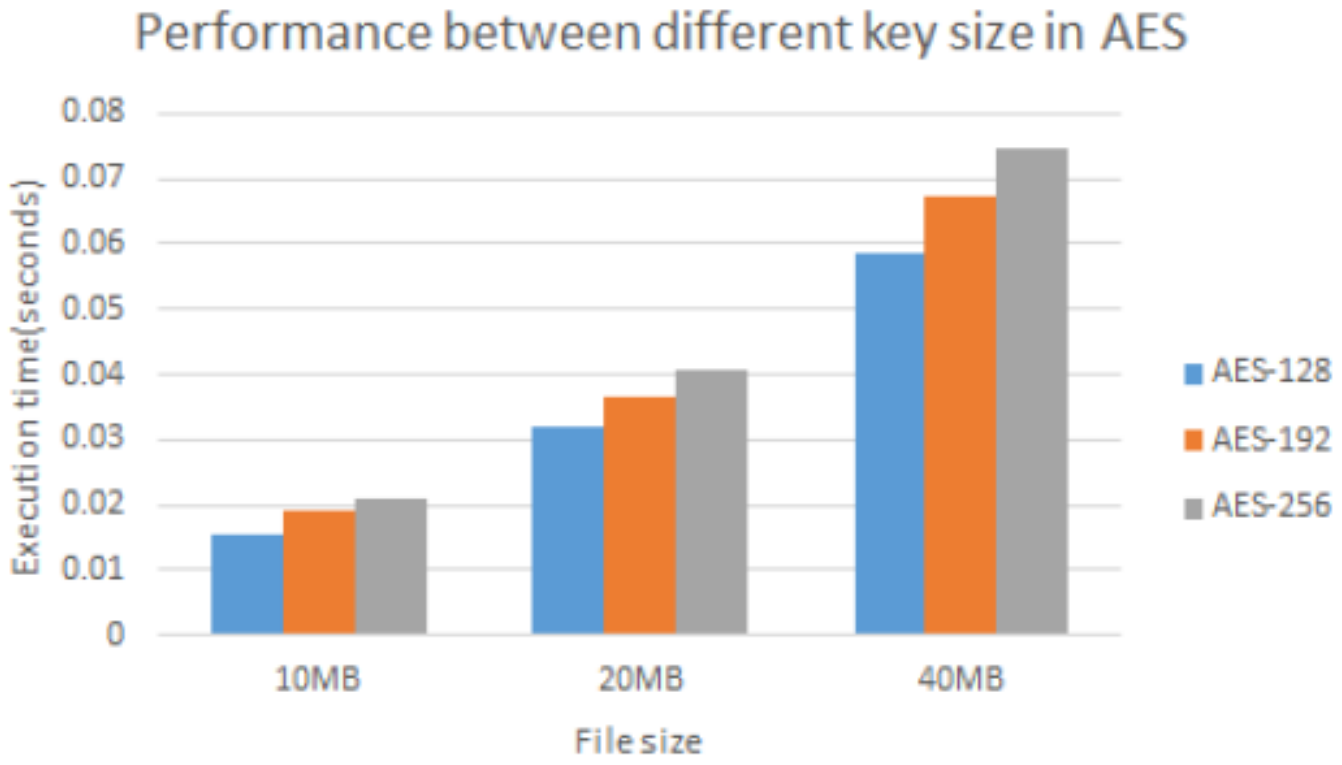
Performance and Evaluation - Quantitative Analysis

- File Encryption and Decryption



Performance and Evaluation - Quantitative Analysis

- File Encryption and Decryption



Conclusions

- A framework using TPA with AES key management to solve the security issues of cloud storage
- An authentication process which is done by the TPA and adoption of the authentication token for double authentication
- A key management scheme which includes storing encryption keys in TPA instead of CSP and the design of master key to protect the encryption keys in TPA

Conclusions

- Two types of key loading methods are proposed to handle frequent key insertions and searches
- The load of the system is well spread between three components to create a system with balanced load
- AES encryption algorithm is adopted to ensure not only security but also performance
- The analyses validate the security, the computational load and the performance of the proposed scheme

Q & A