Information security in cloud service with third party administration

Shivaprasad N ,Prof. Padma Priya

Student, Department of MCA, AMC Engineering College(VTU), Bengaluru, India

Professor ,Department of MCA, AMC Engineering College(VTU), Bengaluru, India

Abstract

Due to the absence of physical control over data in cloud storage, maintaining data integrity becomes a complex problem for customers. Existing techniques like "provable data possession" and "proofs of retrievability" aim to tackle this issue but are primarily designed for auditing static archive data, lacking support for dynamic data changes. Moreover, these schemes often assume an honest data owner and focus on detecting dishonest cloud service providers, neglecting the possibility of customer misbehavior.

This research introduces a novel public auditing approach that addresses data dynamics and ensures fair resolution of disagreements. To overcome the limitation of index utilization in tag calculation observed in current schemes and facilitate efficient management of data dynamics, an index switcher was developed. Additionally, in order to prevent any party from engaging in malicious behavior without detection, the study expands existing threat models and employs a signature exchange approach to construct fair arbitration procedures capable of impartially resolving potential disputes.

The security analysis indicates that our approach is likely to be secure, while the performance assessment demonstrates that the overhead associated with data dynamics and dispute arbitration is manageable.

Overall, this research presents an innovative solution that enables public auditing, supports data dynamics, and incorporates fair arbitration mechanisms to ensure the integrity and reliability of outsourced data in cloud storage environments

1. INTRODUCTION

The cloud computing market is currently undergoing remarkable growth, providing us with unprecedented benefits and opportunities. It revolutionizes virtualization and simplifies the deployment of models like client/server architectures. Cloud computing offers a wide range of services, including distributed computing, grid computing, utility computing, and autonomic computing. Additionally, it provides software services and web services, granting users access to a diverse set of facilities and resources.

The simplicity of operation, cost efficiency, and availability to both individuals and businesses make cloud computing an attractive solution. It leverages Service-Oriented Architecture (SOA) and virtualization technologies to enhance its capabilities. A common practice involves outsourcing services to third-party providers like Amazon, which has evolved into the world's largest online book retailer.

While cloud computing brings numerous advantages, security concerns are inevitable, especially when dealing with on-demand services and virtualization. Although the cloud does offer security measures across different levels, it is not without its flaws. Issues such as inadequate security controls and access management, the potential for insecure data transmission over the network, and the access of different virtual machines to sensitive information pose security risks. As a result, many clients express apprehension when adopting cloud computing due to the potential consequences of these vulnerabilities.

Overall, while cloud computing offers significant benefits and opportunities, it is crucial to address and mitigate the security concerns associated with the technology. By implementing robust security measures, such as encryption, access controls, and monitoring systems, the risks can be minimized, allowing users to fully leverage the advantages of cloud computing while ensuring the safety of their data and operations.

11. Literature Survey:

EXISTING SYSTEM AND

PROPOSED SYSTEM

EXISTING SYSTEM

Most of the existing protocols rely on either public key infrastructure or precise identification, which lack the necessary flexibility for effective key management. In previous versions of the information integrity auditing system, users were required to provide authenticators for data blocks using their own personal keys. This approach places the responsibility on the user to securely store and manage their private key. However, if the user forgets their password or misplaces their hardware token, they will be unable to generate an authenticator for any new data block.

In the event that attackers attempt to access the data owner's files, it is crucial to ensure that the system remains unaware of the specific information related to the attackers. This protects the privacy and confidentiality of the attackers' details.

PROPOSED SYSTEM

When it comes to ensuring victimization prevention, an advanced de-duplication system that supports authorized duplicate checks plays a crucial role. In this new system, a hybrid cloud architecture is employed to facilitate data duplication, thereby enhancing clarity and effectiveness.

To maintain security, private privilege keys are not directly issued to users. Instead, the responsibility of generating and managing these keys lies with the private cloud server. This approach ensures that users cannot disclose their private privilege keys within the context of this system. It effectively prevents users from sharing their privilege keys in more complex environments or settings.

To obtain a file token, users are required to send an invitation to a non-public cloud server. This process ensures that only authorized parties can access the file token, as it is not open to the general public. This added layer of control enhances security and restricts access to authorized users only.

LITERATURE REVIEW:

Title: Ensuring Data Completeness in Remote Servers through Integrity and Internal Control in Information Systems

Authors: Y. Deswarte, J. J. Quisquater, and
A. Saidane

In this study, we address the challenge of verifying the completeness of data stored on remote servers. The integrity checks performed on these servers are susceptible to successful attacks by malicious hackers, rendering their outcomes untrustworthy. However, downloading the data to the validating host is not a practical solution. To overcome this, two alternative approaches based on challenge-response procedures have been proposed.

Title: Analyzing Data to Detect Coordinated Attacks and Probes

Authors: John Green, David Marchette,
Stephen Northcutt, Bill Ralph

This research focuses on multiple networks that have been targeted by coordinated attacks and probes. We provide an explanation of the methods and motives behind these attacks, as well as a description of some specific attack techniques. Additionally, we offer recommendations for identifying and mitigating these coordinated attacks, presenting various analytical techniques.

Title: Privacy-Preserving Public Auditing Protocol for Low-Performance End Devices in Cloud Computing

Authors: J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong

Cloud storage offers extensive storage capacity for both individual and business users. How ever, ensuring data integrity when using cloud storage poses challenges. Existing privacy-preserving public auditing protocols assume that users' end devices have sufficient computational power to perform realtime procedures. In reality, many end devices may have limited computational capabilities. This research presents two efficient public auditing techniques that protect users' privacy without compromising performance. By utilizing online and offline signatures, these protocols enable end devices to perform simple computations only when the data to be outsourced is available. **Fig[1] System Architecture**

V. IMPLEMENTATION MODULES:

Data User:

Register: Provide personal information for registration.

Login: Authenticate user credentials and authorize TPA access.

Upload File: Encrypt and upload files to the cloud server.

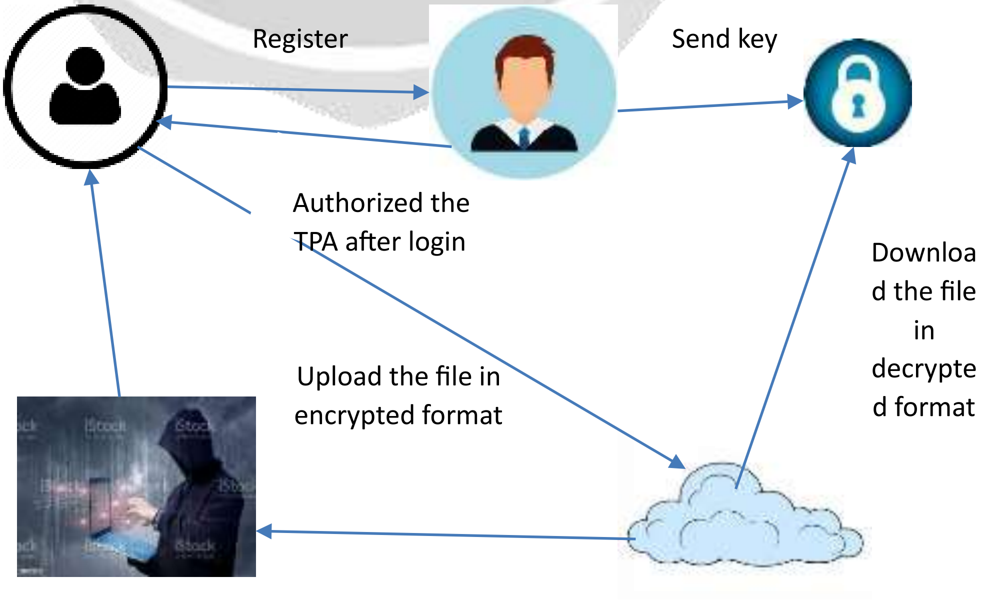
Manage Files: Perform file management operations such as deletion.

Audit File: Initiate a request for file auditing.

View All Files: Access a list of all uploaded files.

Logout: End the user session.

TPA:


Register
Send key
Authorized the TPA after login
Download the file in decrypted format
Upload the file in encrypted format

Login (Username: TPA, Password: TPA): Authenticate TPA access.

View All Users: Access a list of all registered users and their details.

Authorize Users: Grant authorization to users as required.

View Auditing Check Requests: Check incoming file auditing requests.

Respond to Requests: Evaluate the file's integrity and send a response to the user's email.

Logout: End the TPA session.

Cloud:

Login (Username and Password): Authenticate cloud access.

View Users: Access a list of all registered users.

View Uploaded Files: Check all files uploaded by users.

View Auditing Requests: Review pending file auditing requests.

Graph: Generate and display graphs related to system attributes, such as authorized and unauthorized users and request statistics.

Logout: End the cloud session.

KGC (Key Generation Center):

Login with Correct Credentials.

View User Requests: Access requests from users and process key generation.

Send Key: Generate and send encryption keys to authorized users.

Logout: End the KGC session.

Attacker:

Login: Gain unauthorized access.

View All Files: Unauthorized access to view files.

Logout: End the session.

Note: It is essential to ensure that unauthorized access attempts by attackers are prevented or detected and appropriate security measures are in place to protect user data.

V1. CONCLUSION

This article explores various security solutions aimed at ensuring trustworthiness in third-party services, including private clouds, the publication of web documents using XML, initial authentication processes, and authorization mechanisms. One key recommendation is the use of cryptography techniques to encrypt and decrypt sensitive data both on the client and server sides. It is highlighted that the involvement of a reliable third party can greatly enhance the security of cloud services.

The primary objective emphasized in this article is the establishment of a secure and dependable third-party entity to safeguard cloud data. It is essential for users to be proactive in understanding the potential risks associated with their data, privacy, and overall security. By staying informed and taking necessary precautions, users can play an active role in ensuring the protection of their data in the cloud environment.

REFERENCES

[1] International Telecommunication Union, X-509 | ISO/IEC 9594-8, The directory: Public-key and attribute certificate frameworks, ITU, X-Series, 2001. [Citation needed] International Telecommunication Union.

[2] As per The NIST Definition of Cloud Computing, published by the Information Technology Laboratory of the National Institute of Standards and Technology in 2009.

Shen, E., Shi, E., and Waters, B. Privacy Preservation in Encryption Systems. [3] Shen, E., Shi, E., and Waters, B. In TCC.
2009.

[4] Bethencourt, J., Shi, E., Chan, H., Song,

D., and Perrig, A. Performing MultiDimensional Range Queries on Encrypted Data. 2007. Presented at the IEEE Symposium on Security and Privacy.

[5] Song, D., Wagner, D., and Perrig, A.

Practical Techniques for Searching Encrypted Data. Presented at the IEEE Symposium on Research in Security and Privacy in the year 2000.

[6] Boneh, B., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. Public Key Encryption with Keyword Search. Boneh, B., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. 2004 edition of EUROCRYPT.