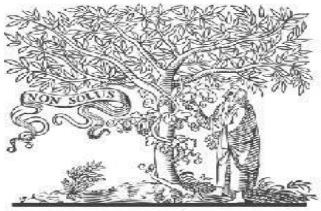
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 31st Mar 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 03

10.48047/IJIEMR/V12/ISSUE 03/87

Title **SECURE DATA DEDUPLICATION USING CP-ABE FOR CLIENT - SIDE CLOUD STORAGE**

Volume 12, ISSUE 03, Pages: 601-605

Paper Authors
Mrs. Pavani.Ch, Saritha Vani. K, Lavanya. V, Tauseeq Shabnam.Sk

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Secure Data Deduplication Using CP-ABE for Client - Side Cloud Storage

Mrs. Pavani.Ch[1], Assistant Professor, Department of Computer Science, Andhra Loyola Institute of Engineering and Technology, Vijayawada.
Saritha Vani. K[2], IV B. Tech Department of Computer Science, Andhra Loyola Institute of Engineering and Technology, Vijayawada.
Lavanya. V[3], IV B. Tech Department of Computer Science, Andhra Loyola Institute of Engineering and Technology, Vijayawada.
Tauseeq Shabnam.Sk[4], IV B. Tech Department of Computer Science, Andhra Loyola Institute of Engineering and Technology, Vijayawada.

Abstract
Now a days, cloud servers such as Google Cloud Platform and Microsoft Azure are widely used to store data, but sometimes storage becomes a problem. It is crucial to ensure data security and confidentiality for private companies and hospitals. To address this, Secure Data Duplication Using CP-ABE For Client-Side Cloud Storage is proposed, which provides both security and deduplication in the cloud. The proposed system uses the CP-ABE algorithm to encrypt user's data with their attributes before uploading it to the cloud, thus ensuring data security. It also checks for file duplication to free up storage space in the cloud. Compared to existing schemes, the proposed system provides a good balance between storage space efficiency and security in a cloud environment, making it suitable for the hybrid cloud model.

Keywords: Confidentiality, Deduplication.

Introduction

Cloud storage has made it easier for data providers to store their data in the cloud while maintaining data privacy through encryption and access control policies. However, the increasing amount of data stored in the cloud requires effective data management techniques such as deduplication to eliminate duplicate data copies. In a corporate setting. employees have varying levels of access based on their department or job role, making it crucial for access control policies to be integrated with data deduplication processes. Existing secure deduplication methods do not allow for access-policy based encryption, which is necessary to limit cloud access to encrypted data. To address this problem, this study proposes Secure data deduplication using CP-ABE for Client-Side cloud storage.

The proposed system enables client-side deduplication and confidentiality through client-side encryption, protecting sensitive data from exposure on untrusted cloud servers. It also includes authorized convergent encryption, which allows only authorized personnel to access critical data. The proposed system provides a suitable balance between storage space efficiency and cloud security, making it appropriate for the hybrid cloud model in a corporate setting. Cloud computing has three primary service models, which are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). These models offer varying levels of control and abstraction over cloud infrastructure, allowing users to build, deploy, and consume applications and services.

An end user layer completes these models, providing a consistent interface for users to access cloud services.

When a user accesses services on the infrastructure layer of the cloud, they have the ability to run their own applications on the cloud infrastructure's resources. However, the user is also responsible for supporting, maintaining, and securing their applications themselves. On the other hand, if the user accesses services on the application layer of the cloud, these tasks are typically

handled by the cloud service provider, without requiring the user to worry about them. This allows the user to focus on their core business tasks, while the cloud provider takes care of the technical details of the application layer

Literature Survey

Paper: Secure and constant cost public cloud storage auditing with deduplication
Author: J. Yuan and S. Yu
Analysis: Cloud storage requires data integrity and storage efficiency. Proof of Retrievability (POR) and Proof of Data Possession (PDP) ensure data integrity, while Proof of Ownership (POW) enhances storage efficiency by securely eliminating duplicated data on the storage server. However, combining POR and PDP can lead to duplication of metadata, which conflicts with the objectives of POW. Existing solutions have computational and communication costs and are insecure. Therefore, this paper proposes a novel scheme based on polynomial-based authentication tags and homomorphic linear authenticators that allows for secure and efficient data integrity auditing with storage deduplication for cloud storage. The proposed scheme allows for deduplication of files and their corresponding authentication tags, achieving data integrity auditing and storage deduplication simultaneously.
Paper: Server aided encryption for deduplicated storage
Author: S. Keelvedhi, M. Bellare, T. Ristenpart.
Analysis:
It is a system and it provides secure deduplicated storage with strong confidentiality guarantees. The system addresses the tension between deduplication and encryption in cloud storage systems by enabling clients to encrypt their data under message-based keys obtained from a key-server via an oblivious PRF protocol. This allows clients to store encrypted data with a storage service, have the service perform deduplication, and yet achieve strong confidentiality guarantees. The system is designed to resist brute-force attacks, and its encryption for deduplicated storage achieves performance and space savings similar to that of using the storage service with plaintext data.
Paper: Proofs of ownership in remote storage system.
Author :S. Halevi, D. Harnika, B. Pinkas and A. Shulman-peleg.
Analysis :
The authors introduce a model for provable data possession (PDP) that enables a client to verify that the server has the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which reduces I/O costs. The client retains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small amount of data, reducing network communication. The PDP model supports large datasets in widely-distributed storage systems.

System Requirement

A. Software Specifications:

The functional requirements or the overall description documents include the product perspective and features, operating system and operating environment, graphics requirements, design constraints, and user documentation.
The appropriation of requirements and implementation rules that gives the general overview of the project in regards to what the areas of strength and deficit. how to tackle them**.**

•Operating System: Windows family
•Coding Language : JSP
•IDE : Netbeans 7.4
•Data Base : MYSQL
•Connectivity : JDBC

B. Hardware Specifications:

Minimum hardware requirements are very dependent on the particular software being developed by a given idea Python /Java/ Canopy / VS Code user. Applications that need to store large arrays/objects in memory will require more RAM, whereas applications that need to perform numerous calculations or tasks more quickly will require a faster processor.

- Processor : minimum intel i3
- Ram : minimum 4 GB

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

- Hard disk : minimum 250GB

Proposed System: The paper uses two secure systems, SecCloud and SecCloud+, to ensure data integrity and deduplication in the cloud. The SecCloud system includes an auditing entity that assists clients in generating data tags before uploading and ensures the integrity of stored data. Seccloud+ enables the guarantee of the confidentiality.
If a user wants to store the data in the cloud he/she should register first then she should login. After logging process the cloud will generate a token. Before uploading files into cloud he should enter his token, if the token entered by the user is valid then he is an authorized person and he's allowed to do actions like upload files, download files. If a user wants to upload a file which is already existed in the cloud then auditor will check the duplicate files and stops uploading such type of file into cloud. If the file is not existed then the data will be encrypted by the CP-ABE algorithm to provide security for the user data. User can also download the other files if he is having the private and public keys of that particular file.

Technology Description
A. Cloud Storage:
Cloud storage has made it easier for data providers to store their data in the cloud while maintaining data privacy through encryption and access control policies. However, the increasing amount of data stored in the cloud requires effective data management techniques such as deduplication to eliminate duplicate data copies. In a corporate setting. employees have varying levels of access based on their department or job role, making it crucial for access control policies to be integrated with data deduplication processes. Existing secure deduplication methods do not allow for access-policy based encryption, which is necessary to limit cloud access to encrypted data.

B. CP-ABE:

The concept of Attribute Based Encryption (ABE), introduced by Sahai and Waters, is a public key cryptography algorithm that enables the encryption of data based on a set of attributes. ABE schemes can be divided into two types: Ciphertext-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE). In KP-ABE schemes, the ciphertext is linked to a set of attributes, while the user's private key is generated based on their corresponding access policy**.** In contrast, CP-ABE schemes associate a user's private key with a set of attributes, and ciphertext is encrypted under a specified access structure. To decrypt a ciphertext, a user must have attributes associated with the ciphertext/private key that satisfy the access policy related to their private key/ciphertext.

Implementation

Figure1: Homepage

In the above picture we can see user interface.

Figure2: Admin Login

In the above screen, We can see two fields in the admin login option. Admin needs to

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

login in order to create accounts for the cloud users

Figure3: Server login

Figure4: User Registration

Here we can see user registration form. If a user wants to store his/her data in the cloud first he should register.

Figure5: Uploading files

Figure6: Downloading Files

Here Users can download their files with the help of their public and private key's.

Figure7: Encrypted Data
Here we are going to encrypt the user's data with help of CP-ABE.

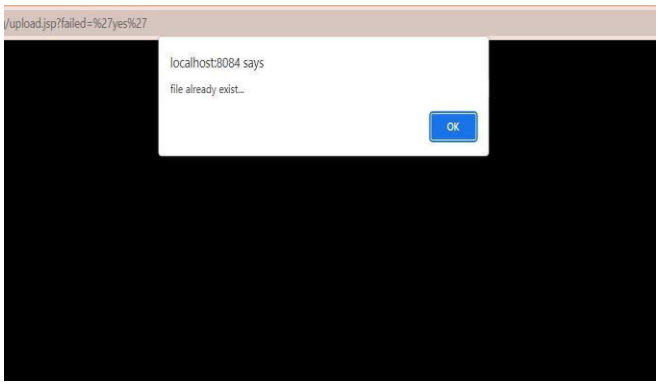


Figure8: Duplicate File

Future implementation

In future work, we aim at deploying our solution in a real environment.

Conclusion

In this research, we proposed a permitted deduplication mechanism based on CP-ABE. The proposed approach utilizes

client-side encryption and deduplication to protect sensitive user data from being exposed on unreliable cloud servers. We also introduced authorized convergent encryption using CP-ABE to ensure that only authorized users can access sensitive data, unlike previous convergent encryption systems.

The focus of this research was on data security and preventing confidential information from leaking. With deduplication, users can save storage in the cloud while also maintaining data confidentiality and integrity.

References

[1] D. Boneh, and M. Franklin, "Identity-based encryption from the Weil pairing," Advances in Cryptology—CRYPTO 2001, Springer Berlin Heidelberg, pp. 213-229, 2001.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology—EUROCRYPT 2005, Springer Berlin Heidelberg, pp. 457-473, 2005.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proceedings of the 13th ACM conference on Computer and communications security, ACM, pp. 89-98, 2006.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," IEEE Symposium on Security and Privacy, IEEE, pp. 321-334, 2007.

[5] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: the essential of bread and butter of data forensics in cloud computing," Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ACM, pp. 282-292, 2010.