International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 6 ; Issue: 7; July- 2024

CryptCloud+: Secure Data Access Control for Cloud Storage

PREETHISHREE A H
PG Student
Department of Master of Computer Application
The Oxford College of Engineering,
Bommanahalli Bengaluru-560068
preethishree2022@gmail.com

DHARAMVIR
Associate Professor
Department of Master of Computer Application
The Oxford College of Engineering,
Bommanahalli Bengaluru-560068
dhiruniit@gmail.com

Abstract — We created Secure Distributed Storage (SDS), a new cloud management system. It is designed to provide easy access to messages while keeping users' identities private. Our system uses the powerful but potentially dangerous CP-ABE (Ciphertext Policy Attribute Based Encryption). A major concern is how access credentials can be misused, as we have seen in cases involving trusted organizations and cloud users. These issues occur whether CP-ABE allows full access or no access. It still uses CP-ABE but adds traceability and auditing capabilities. This development means we can track and identify who has access to data and prevent misuse. Our approach includes detailed security information and real-world examples to demonstrate its benefits.

Keywords: Encryption, Ciphertext, Access, Authorized, Expressive.

INTRODUCTION

The proliferation of distributed computing will create invisible weaknesses in the security of cloud users and the privacy of the information they experience. This is a test specifically designed to ensure that key authorized users can use the cloud[3] to access transported data at any time and from any location. One precaution is to encrypt your data before transferring it to the cloud. But management and information exchange as much as possible. CP-ABE is a powerful encryption tool to protect cloud storage data and protect open access rights. To ensure that only relevant individuals have access to certain information, users are authorized to obtain decryption keys based on their role (e.g. student, employee, guest).. For example, in cases where the school must securely store and store student information in compliance with regulations such as FERPA and HIPAA, the system's senior administrators (such as the security manager) verify the access zone and distribute decryption keys to users. such as students, teachers, staff and researchers

Sensitive student information (such as login information) stored in the cloud can only be accessed by authorized personnel whose responsibility corresponds to decryption capabilities. Internal liability may also arise in the event of misuse, such as unauthorized modification of decryption rights or misuse of information for personal gain. Protecting the integrity of evidence provided by quasi-religious authorities such as school security guards presents another challenge.

Existing System:

Cloud storage has changed the way data is managed, shifting ownership away from traditional data owners as infrastructure and data management is outsourced to cloud providers. This change raises concerns about data privacy management, especially effective planned access controls on the database. Technologies such as search encryption help ensure the security of searching for encrypted files using defined keywords while controlling data and decryption to ensure content authenticity and less retention. For cloud storage systems, especially in asset management environments such as e-health and vehicle networks, it can benefit from the comprehensive storage and availability features of the cloud. However, this integration also brings with it significant security and privacy issues. Attribute-based encryption (ABE), specifically ABE policy (KP-ABE) and ciphertext policy ABE (CP-ABE), solves these problems by allowing attribute management, improving security and efficiency. Despite these advances, issues such as traceability and removal have not yet been resolved. Recent research shows that the CP-ABE role prevents unauthorized distribution of customer collaboration, and the multi-policy CP-ABE architecture allows customers to securely manage their data entries. Technologies such as black box and white box traceability increase accountability in entry standards. Undo the solution. Challenges such as key management, difficult evaluation, and poor implementation should be further investigated. . The goal of these efforts is to strengthen the regulatory framework and reduce risks associated with key management and unauthorized use in the cloud environment.

Proposed System

In our approach to responsible detection and control of malicious cloud users, we use Paillier-like encryption [38] to facilitate accountability. This approach allows us to attribute value to a specific customer based on demand.

1. Detectable: We divide detectability into two types: black-box identification and white-box identification [33]. Black-box identification helps determine who created the decryption device with the correct access keys, while white-box identification indicates who obtained the decryption credentials in the published key. The client's identity is embedded in the certificate using a secret and restricted method similar to Paillier's Removable Role, preventing the client from changing its encoded identity.

2. Audit and Audit : We recommend that access to credentials be double-checked using a decision (such as KeyCheck) to ensure that they are correct during decryption. This helps maintain accurate customer information without requiring additional storage capacity.

3. Agency Accountability: The organization and the customer relationship must agree on the agency’s certification. This ensures that no single authority can control the credentials and that access to the customers credentials remains private. If someone has the right to re-export a registered user's credentials without the user's consent, cryptographic evidence will prove that this right is invalid.

4. Decision Management : To properly manage certificate revocation, we use KeyUpdate to generate updated keys for each revocation. This method involves the use of a linear polynomial (e.g., f(w) = w + 1) to represent the owner's key control and revocation functions to ensure that unauthorized users cannot decrypt newly encrypted data. This approach increases accountability in cloud environments by ensuring that tasks can be traced back to a specific client and prevent unauthorized use or modification of data input. For more information, see Chapters 7 and 8 for details.

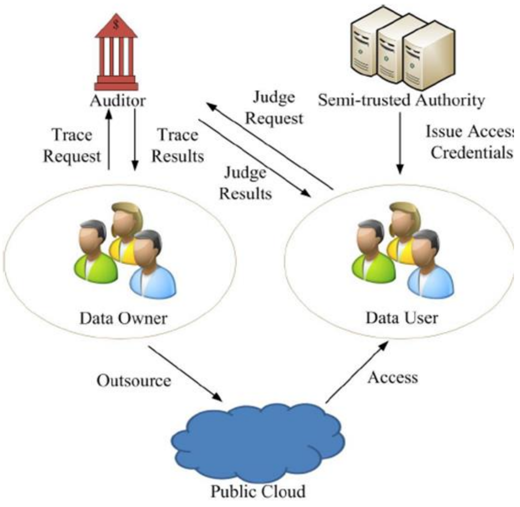


Fig. 1 CP-ABE based cloud storage system.

IMPLEMENTATION

Data Owner: In the data master module, the data manager can perform many important functions: loading data, saving files, sending queries, and getting query results.

This mode allows owners to save content and access certificates. It helps upload encrypted files to protect against unauthorized access. Data owners choose specific data to be sent to cloud servers in encrypted form and retain the ability to search for them effectively. Data owners encrypt their data based on the access code in the data and then outsource it to public cloud servers. Cloud servers store encrypted data provided externally by data owners and process data access requests from authorized data users.

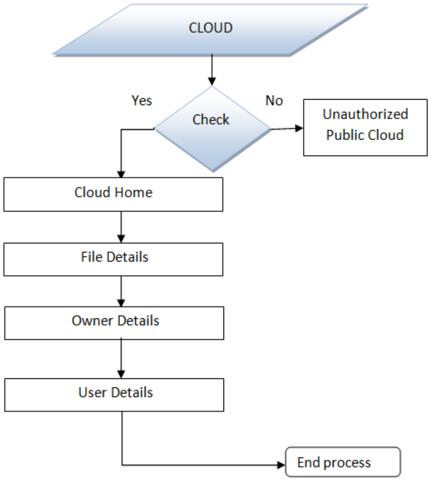


Fig 2 Flow chart

Data User: This module manages customer registration and login information. It allows customers to search for information using multiple keywords, providing accurate results based on queries. Customers can select specific files, save their contents, and receive activation codes via email. After entering the activation code, customers can download and extract the ZIP archive. Data authorization users can access the data owner's data. A semi-trusted authority (STA) creates conflicting and problematic access to credentials such as decryption keys for user data.

Auditor:

Analysts (AUs) are trusted by other organizations to manage and reject ideas. The AU communicates monitoring and auditing results to the Data Owner (DO) and Data Users (DU). In this model, auditors have the option to access the data content and the client requests the content back.

Cloud Server and Encryption Module: This module helps the server to encrypt data using RSA algorithm and convert the encrypted data into ZIP files with activation codes. The activation code is then transferred to the user for download. Cloud servers store the data archive for the data owner. After the cloud server receives the trapdoor (TD) from the user's data, it performs a search and returns the encrypted data at the top.

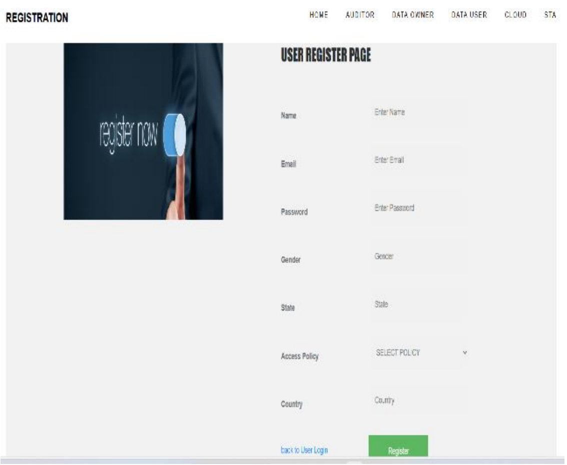


Figure : User registration

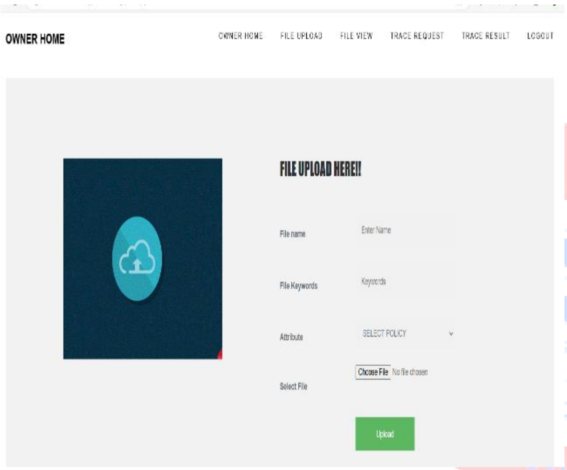
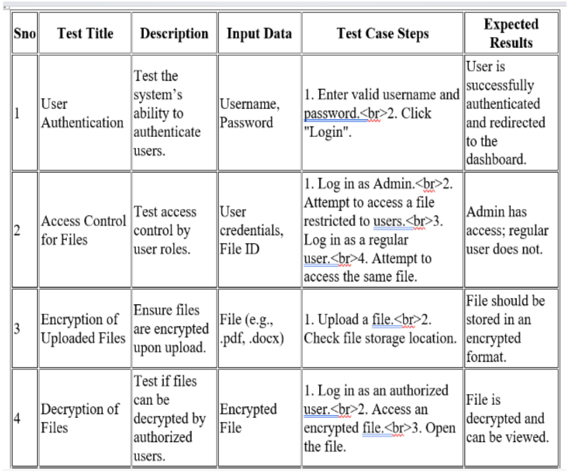


Figure : File upload

TEST CASE



Sno	Test Title	Description	Input Data	Test Case Steps	Expected Results
1	User Authentication	Test the system's ability to authenticate users.	Username, Password	1. Enter valid username and password. 2. Click "Login".	User is successfully authenticated and redirected to the dashboard.
2	Access Control for Files	Test access control by user roles.	User credentials, File ID	1. Log in as Admin. 2. Attempt to access a file restricted to users. 3. Log in as a regular user. 4. Attempt to access the same file.	Admin has access; regular user does not.
3	Encryption of Uploaded Files	Ensure files are encrypted upon upload.	File (e.g., .pdf, .docx)	1. Upload a file. 2. Check file storage location.	File should be stored in an encrypted format.
4	Decryption of Files	Test if files can be decrypted by authorized users.	Encrypted File	1. Log in as an authorized user. 2. Access an encrypted file. 3. Open the file.	File is decrypted and can be viewed.

Table : Test cases for authentication

RESULT

In this study, we solve the access problem in CP-ABE-based cloud storage systems by creating a management role and removing CryptCloud. The system supports white box traceability and auditing. CryptCloud is the first cloud storage solution according to CP-ABE, providing white box traceability, accountability, auditing and efficient deletion. It can monitor and remove malicious users who leak credentials. Our approach can also be applied to cases where user credentials are partially returned by trusted authorities.

CONCLUSION AND FUTURE WORK

In this work, we address the challenges of document authentication in CP-ABE-based cloud storage systems by developing CryptCloud+, a role, authorization, and deletion challenge that integrates free column traceability and auditing. CryptCloud+ is the first CP-ABE-based cloud storage solution that simultaneously provides free text editing, accountability, auditing capabilities, and effective deletion procedures. It has the unique ability to detect and prevent malicious users who leave their credentials. One way to solve this dependency problem is to use multiple authorities (AUs), similar to the first system, which requires good communication and coordination to deal with block AU collision. Other ideas include ensuring multiparty operation to prevent malicious attacks, but this can be difficult. Future research will focus on developing multi-agent computation methods when determining the reliability of AUs without sacrificing stability and performance. As a removable contract, a removable contract is theoretically allowed to provide free-box traceability. Our goal is to increase the effectiveness of follow-up decision-making by striving to achieve the necessary commitment to the partnership. Additionally, CryptCloud+ requires a master key based on the input of the tracking algorithm to enable white-box tracking of malicious cloud users.

REFERENCES

[1] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404, 2017.

[2] Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. IEEE Internet of Things Journal, 4(1):75–87, 2017.

[3] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Advances in Cryptology - EUROCRYPT 2015, pages 595–624, 2015.

[4] Angelo De Caro and Vincenzo Iovino. jpbc: Java pairing based cryptography. In ISCC 2011, pages 850–855. IEEE, 2011.

[5] Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang, and Wenchang Shi. Who is touching my cloud. In Computer Security-ESORICS 2014, pages 362–379. Springer, 2014.

[6] Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasilakos, and Ching-Nung Yang. Enabling semantic search based on conceptual graphs over encrypted outsourced data. IEEE Transactions on Services Computing, 2016.

[7] Vipul Goyal. Reducing trust in the PKG in identity-based cryptosystems. InAdvancesinCryptology-CRYPTO2007, pages430–447. Springer, 2007.