2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

PRIVACY CLOUD SECURE AND EFFICIENT DATA SHARING CONTROL FOR CLOUD STORAGE

[1]P.SHIRISHA, [2]MR B.RAJU

[1] PG Student, Department of Computer Science and Engineering, Chaitanya institute of technology and science Kishanpura,Hanamkonda,Warangal -506001, (.TS).india

[2]Assistant Professor, Department of Computer Science and Engineering ,Chaitanya institute of technology and sciencekishanpura,Hanamkonda,Warangal -506001, (TS).india

[1]palleboinashirisha99@gmail.com,[2]braju1423@hotmail.com

Abstract:

Secure cloud storage, which is an emerging cloud service, is designed to protect the confidentiality of outsourced data but also to provide flexible data access for cloud users whose data is out of physical control. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques that may be leveraged to secure the guarantee of the service. However, the use of CP-ABE may yield an inevitable security breach which is known as the misuse of access credential (i.e. decryption rights), due to the intrinsic "all-or-nothing" decryption feature of CP-ABE. In this paper, we investigate the two main cases of access credential misuse: one is on the semi-trusted authority side, and the other is on the side of cloud user. To mitigate the misuse, we propose the first accountable authority and revocable CP-ABE based cloud storage system with white-box traceability and auditing, referred to as CryptCloud+. We also present the security analysis and further demonstrate the utility of our system via experiments.

.

I.INTRODUCTION

The predominance of cloud computing may in a roundabout way cause of the helplessness to the privacy of outsourced data furthermore, the protection of cloud clients. A specific test here is on the most proficient method to ensure that exclusive approved clients can pick up access to the data, which has been outsourced to cloud, at anyplace and whenever. One credulous arrangement is to utilize encryption system on the data before uploading to cloud. Yet it limits data sharing scheme.Thisis so in light of the fact that a data proprietor needs to download the encrypted data from cloud and further re-scramble them for sharing (assume the data proprietor has no nearby duplicates of the data). A fine-grained get to control over encrypted data is alluring with regards to cloud computing. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) might be an effective answer for ensuring the confidentiality of data and to give fine-grained access control here. In a CP-ABE based cloud storage framework, for instance, associations and people can first specify access policy over attributes of a potential cloud client. Approved cloud clients at that point are conceded access credentials (i.e., decryption keys) corresponding to their attributesets which

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

can be utilized to get access to the outsourced data. CP-ABE offers a dependable strategy to protect data put away in cloud, yet likewise empowers fine-grained access control over the data. Any information that is stored in cloud if leaked, could result in arange of consequences for the association and people. The existing CP-ABE based[1] schemeenables us to keep security breach from outside attacker and also an insider of the association who commits the "crimes" of redistributingthe decryption rights and the circulation of understudy data in plain arrangement for illicit financial picks ups. At the same time, it can also ensure that semi-trusted authority won't (re-)distribute the created access credentials to others by proposing CryptCloud+, which provided an accountable authority and revocable CP-ABE based cloud storage system. In any case, one trying issue in taking care of client disavowal in cloud storage is that a revoked client may in any case will still have the capacity to unscramble an old ciphertext they were approved to access before being revoked. To address this issue, the ciphertext put away in the cloud storage ought to be updated, preferably by the (untrusted) cloud server. Also it lacked timed data accessing control which would provide a substantial level of security.

II.EXISTING SYSTEM:

- In a CP-ABE based cloud storage system, for example, organizations (e.g., a university such as the University of Texas at San Antonio) and individuals (e.g., students, faculty members and visiting scholars of the university) can first specify access policy over attributes of a potential cloud user.
- Authorized cloud users then are granted access credentials (i.e., decryption keys) corresponding to their attribute sets (e.g., student role, faculty member role, or visitor role), which can be used to obtain access to the outsourced data.
- As a robust one-to-many encryption mechanism, CP-ABE offers a reliable method to protect data stored in cloud, but also enables fine-grained access control over the data.

Disadvantages of Existing System:

- The leakage of any sensitive student information stored in cloud could result in a range of consequences for the organization and individuals (e.g., litigation, loss of competitive advantage, and criminal charges).

The existing CP-ABE based cloud storage systems fail to consider the case where access credential is misused

III.PROPOSED SYSTEM:

Seeking to mitigate access credential misuse, we propose CryptCloud+, an accountable authority and revocable CPABE based cloud storage system with white-box traceability and auditing.

Specifically, in our work, we first present a CP-ABE based cloud storage framework. Using this (generic) framework, we propose two accountable authority and revocable CP-ABE systems (with whitebox traceability and auditing) that are fully secure in the standard model, referred to as ATER-CP-ABE and ATIR-CPABE,

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


respectively. Based on the two systems, we present the construction of CryptCloud+ Access credentials for individual traced and further determined to be "compromised" can be revoked..

Advantages of Proposed System:

- To the best of our knowledge, this is the first practical solution to secure fine-grained access control over encrypted data in cloud.
- Users who leak their access credentials can be traced and identified.
- A semi-trusted authority, who (without proper authorization) generates and further distributes access credentials to unauthorized user(s), can be identified. This allows further actions to be undertaken (e.g. criminal investigation or civil litigation for damages and breach of contract).
- An auditor can determine if a (suspected) cloud user is guilty in leaking his/her access credential.

IV.IMPLEMENATATION:

Data Owner:

In the first module, we develop the Data Owner Module. In this module, data owner has the option of File Upload, File View, Trace Request and Trace Results. This module helps the owner to register those details and also include login details. This module helps the owner to upload his file with encryption algorithm. This ensures the files to be protected from unauthorized user. Data owner has a collection of documentsthat he wants to outsource to the cloud server in encrypted form while still keeping the capability to search on them for effective utilization. Data Owners (DOs) encrypt their data under the relevant access policies prior to outsourcing the (encrypted) data to a public cloud (PC). PC stores the outsourced (encrypted) data from Dos and handles data access requests from data users (DUs)

Data User:

This module includes the user registration login details. This module is used to help the client to search the file using the multiple key words concept and get the accurate result list based on the user query. The user is going to select the required file and register the user details and get activation code in mail email before enter the activation code. After user can download the Zip file and extract that file. Data users are authorized ones to access the documents of data owner. With t query keywords, the authorized user can generate a trapdoor TD according to search control mechanisms to fetch k encrypted documents from cloud server. Then, the data user can decrypt the documents with the shared secret key. Authorized DUs are able to access (e.g. download and decrypt) the outsourced data.

Semi-trusted authority:

Semi-trusted authority (STA) generates system parameters and issues access credentials (i.e., decryption keys) to DUs.

Auditor:

Auditor (AU) is trusted by other entities, takes charge of audit and revoke procedures, and returs the trace and audit results to DOs and DUs. In this module, auditor has the options of File details, User Request & Trace Request details.

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


Cloud Server and Encryption Module:

This module is used to help the server to encrypt the document using RSA Algorithm and to convert the encrypted document to the Zip file with activation code and then activation code send to the user for download. Cloud serverstores the encrypted document collection for data owner. Upon receiving the trapdoor *TD* from the data user, the cloud server executes search, and finally returns the corresponding collection of top- *k* ranked encrypted documents. Besides, upon receiving the update information from the data owner, the server needs to update and document collection *C* according to the received information. The cloud server in the proposed scheme is considered as "honest-but-curious", which is employed by lots of works on secure cloud data search

CONCLUSION

In this work, we have addressed the challenge of credential leakage in CP-ABE based cloud storage system by designing an accountable authority and revocable CryptCloud which supports white-box traceability and auditing (referred to as CryptCloud+). This is the first CP-ABE based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, CryptCloud+ allows us to trace and revoke malicious cloud users (leaking credentials). Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority.

We note that we may need black-box traceability, which is a stronger notion (compared to white-box traceability), in CryptCloud. One of our future works is to consider the black-box traceability and auditing. Furthermore, AU is assumed to be fully trusted in CryptCloud+. However, in practice, it may not be the case. Is there any way to reduce trust from AU? Intuitively, one method is to employ multiple AUs. This is similar to the technique used in threshold schemes. But it will require additional communication and deployment cost and meanwhile, the problem of collusion among AUs remains. Another potential approach is to employ secure multi-party computation in the presence of malicious adversaries. However, the efficiency is also a bottleneck. Designing efficient multi-party computation and decentralizing trust among AUs (while maintaining the same level of security and efficiency) is also a part of our future work. We use Paillier-like encryption to serve as an extractable commitment to achieve white-box traceability. From an abstract view point, any extractable commitment may be employed to achieve white-box traceability in theory. To improve the efficiency of tracing, we may make use of a more light-weight (pairing-suitable) extractable commitment.

Also, the trace algorithm in CryptCloud+ needs to take the master secret key as input to achieve white-box traceability of malicious cloud users. Intuitively, the proposed CryptCloud+ is private traceable5. Private traceability only allows the tracing algorithm to be run by the system administrator itself, while partial/full public traceability enables the administrator, authorized users and even anyone without

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

the secret information of the system to fulfill the trace. Our future work will include extending CryptCloud+ to provide "partial" and fully public traceability without compromising on performance.

VI.REFERENCES:

[1] Mazhar Ali, RevathiDhamotharan, 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] Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.

[4] NuttapongAttrapadung and Hideki Imai.Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278–300. Springer, 2009.

[5] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[6] MihirBellare and OdedGoldreich.On defining proofs of knowledge. In Advances in Cryptology-CRYPTO'92, pages 390–420. Springer, 1993.

[7] Dan Boneh and Xavier Boyen.Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.

[8] HongmingCai, BoyiXu, 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.

[9] 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.

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

[11] 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.

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

[13] VipulGoyal. Reducing trust in the PKG in identity based cryptosystems. In Advances in Cryptology-CRYPTO 2007, pages 430–447. Springer, 2007.

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

[14] VipulGoyal, Steve Lu, AmitSahai, and Brent Waters. Black-box accountable authority identity-based encryption. In Proceedings of the 15th ACM conference on Computer and communications security, pages 427–436. ACM, 2008.

[15] VipulGoyal, OmkantPandey, AmitSahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98. ACM, 2006.