Cipher text Classification using ABE Method in Audit-Free Cloud Storage

[1]Samanthula Chinnama Naidu, [2]K Satyanarayana Murthy

[1,2]Dept. of CSE, Baba Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh, India

Abstract

Cloud storage offerings have come to be increasingly across the board. In light of the fact that of the estimation of privations, many cloud storage encryption plans have been proposed to shield information from people who don't have section. Every such plan expected that cloud storage merchants are riskless and can't be hacked; in any case, in take after, a few specialists (i.e., coercers) may drive cloud storage suppliers to unveil individual insider facts or private information on the cloud, hence through and through dodging storage encryption plans. In this paper, we exhibit our outline for a fresh out of the box new cloud storage encryption conspire that grants cloud storage suppliers to make persuading counterfeit client privileged insights to take care of client privatives. For the reason that coercers can't reveal if procured mysteries are appropriate or not, the cloud storage provider be sure that client privateers keeps on being safely secured.

Keywords

Cloud Storage, Integrity, Protection Safeguarding, Authenticator Recovery, Intermediary, Auditor

I. Introduction

Cloud storage is a type of information storage where the advanced information is put away in comprehensible pools, the physical storage traverse different servers (and frequently areas), and the physical condition is ordinarily possessed and dealt with by a facilitating association. These cloud storage suppliers are liable for keeping the information accessible and accessible, and the physical condition secured and running. Distinctive associations purchase or rent storage limit from the suppliers to store client application information [1]. Cloud storage administrations might be accessed through a co-found cloud PC benefit, a web benefit application programming interface (API)[2] or by applications that use the API, for example, cloud desktop storage, a portal or Web-based substance administration frameworks. In the cloud storage condition clients can store their information on the cloud and access their information from anyplace whenever by associating with a system [3]. In view of client security, the information put away on the cloud is typically encoded and safe monitored from access by different clients [4]. Thinking about the synergistic property of the cloud information, attribute-based encryption (ABE) is viewed as a standout amongst the most reasonable encryption plans for cloud storage. Attribute-based encryption is a sort of open key encryption in which the mystery key of a client and the ciphertext are dependent upon attributes. In such a structure, the unscrambling of a ciphertext is achievable just if the arrangement of attributes of the client key equivalents the attributes of the ciphertext.[5]. A focal security highlight of Attribute-Based Encryption is conspiracy protection: A challenger that grips various keys should just be skilled to access information if no less than one individual key grants access. The point picking this attribute-based encryption is that as more responsive, information is shared and put away by outsider locales on the Internet, there will be a need to scramble information put away at these destinations. One hindrance of scrambling information is that it can be specifically shared just at a coarse-grained level (i.e., giving another gathering your private key). To conquer this inconvenience we utilized another cryptosystem for fine-grained sharing of encoded information that we call Key-Policy Attribute-Based Encryption (KP-ABE) [6]. In this cryptosystem, ciphertext are marked with sets of attributes and private keys are related with access structures that control which ciphertext by this the client can without much of a stretch ready to unscramble the information which was scrambled. The materialness of this development is to share the audit-log data and communicate encryption and furthermore bolsters designation of private keys which incorporates the Hierarchical Identity-Based Encryption. These Encryption plans guaranteeing that cloud storage specialist organizations or trusted outsiders taking care of key administration are trusted and can't be hacked [7]. Attribute based encryption has been quick created since it was conceived, and it is a hot bearing in cryptograph as of late, which acknowledges non intuitive fine-grained access control system, grows coordinated model to one to many model on encryption and unscrambling, significantly advances the adaptability of encryption strategy and depiction of client consents. Subsequently, it has a decent application prospects in conveyed document administration, outsider information storage, pay TV framework and other fields [5-6]. Nonetheless, in all current ABE plans, all clients can just get one same sort of consent if fulfilling access arrangement. With the fast improvement of system, the ascent of cloud registering and diverse request development of huge scale client, it is important to give clients distinctive consents. Be that as it may, in all current ABE plans, all clients can just get one same sort of authorization if fulfilling access strategy. With the fast improvement of system, the ascent of cloud registering and diverse request development of expansive scale client, it is important to give clients distinctive authorizations. For instance: there are four attribute experts checking four attribute sets.

II. Related Work

A. Fuzzy Identity-Based Encryption

We present another sort of Identity-Based Encryption (IBE) plot that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we see a way of life as set of engaging attributes. A Fuzzy IBE conspire takes into consideration a private key for a personality, ω, to unscramble a ciphertext scrambled with a character, ω ′, if and just if the personalities ω and ω ′ are near each different as measured by the "set cover" remove metric. A Fuzzy IBE plan can be connected to empower encryption utilizing biometric contributions as characters; the mistake resistance property of a Fuzzy IBE conspire is decisively what takes into consideration the utilization of biometric personalities, which naturally will have some clamor each time they are examined. Also, we demonstrate that Fuzzy-IBE can be utilized for a sort of use that we term "attributebased encryption".

B. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

As more touchy information is shared and put away by outsider destinations on the Internet, there will be a need to scramble information put away at these locales. One disadvantage of scrambling information, is that it can be specifically shared just at a coarse-grained level (i.e., giving another gathering your private key). We build up another cryptosystem for fine-grained sharing of encoded information that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, figure writings are marked with sets of attributes and private keys are related with access structures that control which figure messages a client can decode. We show the pertinence of our development to sharing of audit-log data and communicate encryption. Our development underpins designation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

C. Cipher Content Policy Attribute-Based Encryption

In a few disseminated frameworks a client should just have the capacity to access information if a client groups a specific arrangement of certifications or attributes. As of now, the main strategy for authorizing such strategies is to utilize a trusted server to store the information and intervene access control. Be that as it may, if any server putting away the information is traded off, at that point the secrecy of the information will be bargained. In this paper we introduce a framework for acknowledging complex access control on encoded information that we call Cipher content Policy Attribute-Based Encryption. By utilizing our procedures encoded information can be kept secret regardless of whether the storage server is untrusted; additionally, our techniques are secure against conspiracy assaults. Past Attribute-Based Encryption frameworks utilized attributes to portray the scrambled information and incorporated approaches with client's keys; while in our framework attributes are utilized to depict a client's accreditations, and a gathering encoding information decides a strategy for who can decode. In this manner, our techniques are reasonably nearer to conventional access control strategies, for example, Role-Based Access Control (RBAC). Furthermore, we give an execution of our framework and give execution estimations.

D. Cipher Content Strategy Attribute-Based Encryption: An Expressive, Productive and Provably Secure Acknowledgment

We exhibit another system for acknowledging Cipher content Policy Attribute Encryption (CP-ABE) under cement and no intuitive cryptographic suspicions in the standard model. Our answers permit any encryptor to indicate access control as far as any access recipe over the attributes in the framework. In our most effective framework, figure content size, encryption, and decoding time scales straightly with the intricacy of the access equation. The main past work to accomplish these parameters was constrained to a proof in the non specific gathering model. We exhibit three developments inside our system. Our first framework is demonstrated specifically secure under a supposition that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) suspicion which can be seen as a speculation of the BDHE presumption. Our next two developments give execution tradeoffs to accomplish provable security individually under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman suppositions.

E. Dynamic Certifications and Ciphertext Designation for Attribute-Based Encryption

Motivated by the subject of access control in cloud storage, we consider the issue utilizing Attribute-Based Encryption (ABE) in a setting where clients' accreditations may change and ciphertexts might be put away by an outsider. Our fundamental outcome is gotten by blending two commitments: We at that point join these two outcomes for another approach for denial on put away information. Our plan enables a storage server to refresh put away ciphertexts to exclude disavowed clients from accessing information that was encoded before the client's access was denied while key refresh communicates can progressively renounce chose clients.

III. Problem Statement

The cloud user, who has large amount of data files to be stored in the cloud; the cloud server, which is managed by the cloud service provider to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter); the third-party auditor, who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. As users no longer possess their data locally, it is of critical importance for users to ensure that their data are being correctly stored and maintained. To save the computation resource as well as the online burden potentially brought by the periodic storage correctness verification, cloud users may resort to AUDITOR for ensuring the storage integrity of their out sourced data, while hoping to keep their data private from AUDITOR. Using third-party auditing service provides a cost-effective method for users to gain trust in cloud. We assume the AUDITOR, who is in the business of auditing, is reliable and independent. However, it may harm the user if the AUDITOR could learn the out sourced data after the audit[5]. Note that in our model, beyond users' reluctance to leak data to AUDITOR; we also assume that a cloud server has no incentives to reveal their hosted data to external parties.

IV. Third Party Auditor

The audit in cloud computing is broadly classified into three, they are first party auditor or internal auditor where the cloud user organization audits by its own, it is a self-assessment procedure for intrusion detection and prevention system. Second party auditor is a Cloud Service Provider who has significant resources and experts in building and managing distributed cloud storage servers, owns and operates where an external auditing procedure is used for data security and quality management in cloud services. The Cloud data storage architecture consists of three actors, the cloud user who has large amount of data to be stored and retrieved as per the requirement in the cloud. The cloud service provider who maintains the cloud storage services and provides cloud data storage. To enable privacy preserving public auditing for cloud data storage shown in the model, the protocol we designed should achieve the following prevention, protection and performance guarantees;

A. Storage Accuracy

To ensure that the users data are indeed stored appropriately and kept all the time in cloud.

2. Reliable Security

To ensure that the AUDITOR cannot gain users data from the information collected during the auditing process.

3. Group Auditing

To enable AUDITOR provide secure and efficient auditing to possible large number of different users simultaneously

4. Detection and Prevention

To allow AUDITOR to provide auditing with minimum communication.

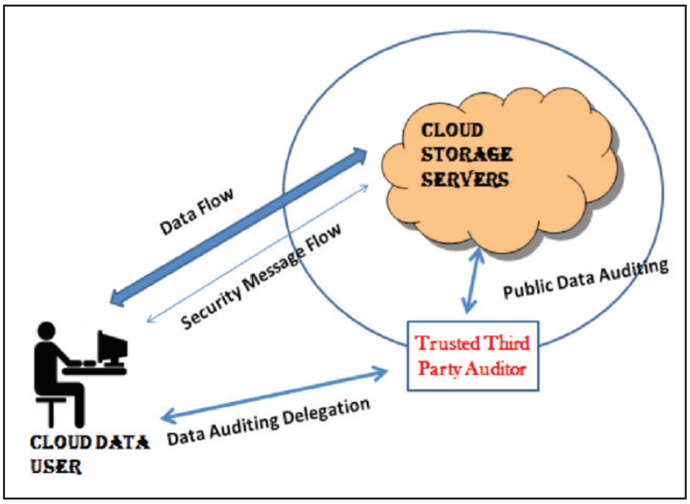


Fig. 1: The Architecture of Cloud Data Storage Services

The Trusted Third Party (TTP) is an audit based organization which facilitates secure interactions between two parties that is cloud user and cloud provider, where both of them trust this third party. The Third Party Auditor (AUDITOR) registered security service provider allocated by the cloud service provider with strong Authentication and Authorization. The AUDITOR can perform Multiple Auditing Tasks for single or multiple clouds in branch manner for better efficiency and security [6].Public audit-ability: to allow AUDITOR to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

V. System Model

A. Cloud Server

A local Cloud which provides priced abundant storage services are been created in this module. The users can upload their data in the cloud. This module can be developed where the cloud storage can be made secure. The cloud is not fully honorable by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to that the cloud server is genuine but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data investigating schemes, but will try to learn the content of the stored data and the identities of cloud users. This essentially means that the owner (client) of the data moves its data to a third party cloud storage server which are supposed to presumably for a fee truly store the data with it and provide it back to the owner whenever required.

The cloud server provides privilege to generate secure multi-owner data sharing scheme called MONA. It denotes that any user in the group can securely share data with others by the cloud. This scheme is able to support dynamic groups comfortably. Respectively, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners but within the group.

B. Proxy Server Deployment

Group manager takes charge of followings,

1. Signature Generation

- Signature Verification
- Content Regeneration

A proxy agent acts on behalf of the data owner to regenerate authenticators and data blocks on the servers during the repair procedure. Notice that the data owner is restricted in computational and storage resources compared to other entities and may become off-line after the data upload procedure. The proxy, who would always be online, is supposed to be much more powerful than the data owner but less than the cloud servers in terms of computation and memory capacity. To save resources as well as the online burden potentially brought by the periodic auditing and accidental repairing, the data owners resort to the AUDITOR for integrity verification and delegate the reparation to the proxy. Considering that the data owner cannot always stay online in practice, in order to other group content he will be revoked by the cloud server.

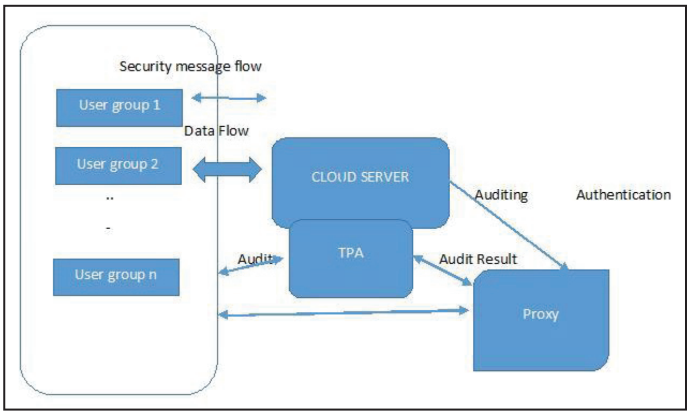


Fig. 2: Cloud Regeneration Architecture

VI. Proposed System Architecture

This paper involves three parties: The cloud server, the third party auditor (AUDITOR) and users is shown in fig. 3. There are two types of users in a group: the original user and a number of group users. The original user and group users are both members of the group. Group members are allowed to access and modify shared data created by the original user based on access control polices. Shared data and its verification information (i.e. Mac code) are both stored in the cloud server. The third party auditor is able to verify the integrity of shared data in the cloud server on behalf of group members.

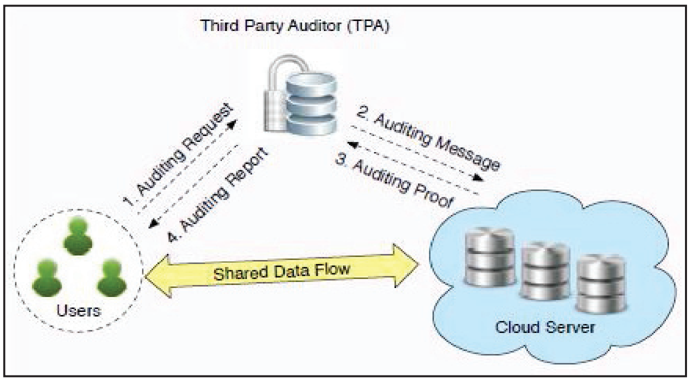


Fig. 3: System Model Includes User, Cloud Server and Auditor

In this paper, we only consider how to audit the integrity of shared data in the cloud with static groups. It means the group is pre-defined before shared data is created in the cloud and the membership of users in the group is not changed during data sharing. The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud. When a user (either the original user or a group user) wishes to check the integrity of shared data, she first sends an auditing request to the AUDITOR. After receiving the auditing request, the AUDITOR generates an auditing message to the cloud server, and retrieves an auditing proof of shared data from the cloud server. Then the AUDITOR verifies the correctness of the auditing proof. Finally, the AUDITOR sends an auditing report to the user based on the result of the verification.

Proposed Algorithm

Authentication, Authorization and Auditing for secure cloud storage is implemented on the basis of the following key points

- Our System Supports an External auditor to audit users outsourced data in the cloud without learning knowledge on the data content.
- The AUDITOR supports scalable on request by cloud service provider for efficient public auditing in the cloud computing
- Auditing is the processes which is done for the cloud to achieve batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the AUDITOR
- The auditing is the intelligence based Dynamic data process for the data and information security in cloud computing
- data integrity algorithm such as Message Authentication Code (MAC code) by means of Hash Based Message Authentication Code (HMAC code) to check the integrity of the data being stored in the cloud.
- By means of MAC code, we enhance the data integrity of the cloud data.

Step 1: Start of an Algorithm
Step 2: Key Generation by Advanced Encryption Standard (AES) Algorithm 16-bit Hexa Decimal keys are generated
Step 3: Map the Key to the files
Step 4: Divide the files into the blocks
Step 5: Each Encrypted Block is Associated with Key
Step 6: Store the data blocks to the Cloud Storage Server
Step 7: Simultaneously Intelligent system sends a copy of keys to AUDITOR
Step 8: On request of Cloud Service Provider (CSP) the Auditing processes with be done by AUDITOR
Step 9: Validate the data by signatures and data integrity proofs
Step 10: Successful validation, verification will be done for dynamic auditing by AUDITOR End of Algorithm.

VII. Conclusion

In this paper, we propose a privacy-preserving public auditing system for data storage security incloud computing. Although the computational time is increased but the privacy is preserved. Where data is stored in the cloud by using the most prominent algorithm AES. We utilize the holomorphic linear authenticator and random masking to guarantee that the AUDITOR would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the load of cloud user from the tedious and possibly expensive auditing task, but also reduces the users fear of their outsourced data leakage. Considering AUDITOR may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where the AUDITOR can perform multiple auditing tasks in a batch manner for better efficiency. We had overcome most of drawbacks of the existing system by securing data dynamics and performance improvement. General analysis shows that our schemes are provably secure and highly efficient. Our preliminary experiment conducted case further demonstrates the fast performance of our design on both the cloud and the auditor side. We leave the full-fledged implementation of the mechanism on commercial public cloud as an important future scope.

References

[1] A. Sahai, B. Waters,“Fuzzy identity-based encryption”, In Eurocrypt, pp. 457–473, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, B. Waters,“Attribute-based encryption for fine-grained access control of encrypted data”, In ACM Conference on Computer and Communications Security, pp. 89–98, 2006.

[3] J. Bethencourt, A. Sahai, B. Waters,“Ciphertext-policy attribute-based encryption”, In IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[4] B.Waters,“Ciphertext-policy attribute-based encryption: An expressive, efficient and provably secure realization”, In Public Key Cryptography, pp. 53–70, 2011.

[5] A. Sahai, H. Seyalioglu, B. Waters,“Dynamic credentials and ciphertext delegation for attribute-based encryption”, In Crypto, pp. 199–217, 2012.

[6] S. Hohenberger, B. Waters,“Attribute-based encryption with fast decryption”, In Public Key Cryptography, pp. 162–179, 2013.

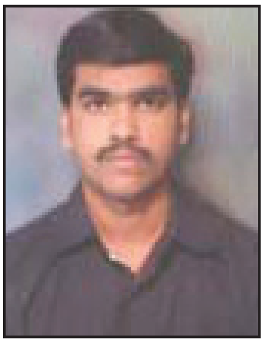
[7] K. Liang, L. Fang, D. S. Wong, W. Susilo,“A ciphertext policy attribute-based proxy re-encryption with chosen-ciphertext security”, IACR Cryptology ePrint Archive, pp. 236, 2013.

[8] Dalia A, Batrafi O.,"Efficient integrity checking technique for securing client data in cloud computing", 2011.

[9] Balakrishnan S, Saranya G, Shobana S, Karthikeyan S., "Introducing Effective Third Party Auditing (AUDITOR) for Data Storage in Cloud", IJCST 2011; 2(2).

[10] M. Armbrust et al.,“Above the clouds: A Berkeley view of cloud computing”, Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009.

Samanthula Chinnama Naidu holds a B.tech certificate in Computer Science Engineering from the University of JNTU Kakinada. He presently pursuing M.Tech (CSE) Department of Computer Science Engineering from Baba Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh, India



K Satyanarayana Murthy is working as an Assistant Professor in the Department of Computer Science and Engineering in Baba Institute of Technology and Sciences. He is having 10 years teaching experience.