Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 10 Issue: 01 | Jan-2025

Analysis of an attribute-based encryption system for cloud data access

[1]Bhavuk Sharma,[2]Dr. Bhupendra Verma, [3]Dr. Vivek Sharma

1M.Tech Scholar

2,3Professor, Department of Computer Science Engineering, Technocrats Institute of Technology, Bhopal, M.P, India

---

Abstract -There is a way to lower the Internet's common overhead and offer a fine-grained access control whenever cloud access control is being considered. These problems can be resolved with attribute-based encryption. A centralized attribute-based encryption scheme is suggested for the current system, in which users get secret keys and attributes from a single key distribution center.This paper suggests a decentralized attribute-based encryption system where any party can function as the authority by generating a public key and providing various users with private keys. Additionally supported by the suggested system are user revocation and anonymous authentication. The performance of decentralized Cipher-text attribute-based encryption and attribute-based encryption can also be compared.

***Key Words*: Cloud Computing, Access control, Key Distribution Center (KDC), Authentication, Revocation, Attribute Based Encryption(ABE)**

1.INTRODUCTION

Currently, cloud computing is a potential computing paradigm that is being widely considered across many domains. A lot of cloud service providers now allow businesses to buy the necessary computer resources rather than setting up and managing their own computing environment.Cloud storage houses a large amount of very sensitive data. The two most crucial concerns in cloud computing are privacy and security. The user should be verified before starting a transaction, but they should also be guaranteed that the cloud won't alter the data they have outsourced. To prevent other users or the cloud from knowing who they are, individuals must maintain their privacy.

The importance of limiting access to legitimate services to authorized users has led to an increase in interest in cloud access control. Clouds hold a vast quantity of data and information, much of which contains sensitive data. In general, there are three forms of access control: Attribute-based access control (ABAC), Role-based access control (RBAC) and User-based access control (UBAC). Users are categorized according to their respective responsibilities in role-based access control. The list of approved users with data access is part of the access control list in user-based access control. Access policy is associated to the data in ABAC, and users who meet the access policy and possess a valid set of characteristics are granted access to the data.Access controls on cloud systems, such as Fine-Grained Data Access Contro, Attribute Based Data Sharing, Hierarchical Attribute Based Encryption and Distributed Access Control are centralized and employ a symmetric key approach, in which all users receive their attributes and secret keys from a single key distribution center (KDC). A single KDC is exceedingly challenging to manage in a cloud environment where many users are supported. The new feature in this study is that it allows the message to be legitimate and genuine without disclosing the name of the person who placed the data on the cloud. This approach may also be extended to user revocation. This work uses the Attribute Based Signature (ABS) technique to ensure privacy and authenticity. Additionally, this approach is immune to replay attacks, in which users may substitute outdated data for the new data. The fact that a revoked user cannot write to the cloud makes this method a crucial feature. The right cryptography technology is used to achieve safe data transactions on clouds. The owner of the data should store it in the cloud after encrypting it. In the event that a third party downloads the record, the user may see it if they possess the key used to rewrite the encrypted data. This might sometimes be a failure due to the programmers and advancements in technology. There are several methods and strategies to create safe transactions and storage in order to solve the issue suggested an anonymous authentication system for cloud data preservation. Anonymous authentication is the process of admitting a user without knowing their personal information. As a result, the user may hide their information from other cloud users since the cloud servers are unaware of their personal information.

1.1 Motivation

There are currently well-known security solutions that primarily rely on authentication to ensure that a user's private data is not illegally accessed, but they overlook a minor privacy concern when a user challenges the cloud server to seek data sharing with other users. The disputed access request itself may disclose the user's privacy. Existing systems describe a shared authority-based privacy-preserving authentication methodology that ensures security and privacy in cloud storage. The shared access authority is obtained using an anonymous access request matching process that takes security and privacy into account. Attribute-based access control is used to ensure that the user can only access its own data fields; the cloud server uses proxy re-encryption to enable data sharing across numerous users.

2. Need of the Study

There are already well-known existing security solutions that specialize in authentication to appreciate that a user's private information cannot be unauthorized accessed, but neglect a refined privacy issue throughout a user difficult the cloud server to request different users for information sharing.

3. Litrature Review

Hong Liu et al. Cloud services provide consumers the ease of enjoying on-demand cloud apps without regard for local infrastructure limits. Existing security solutions mostly rely on authentication to ensure that a user's private data cannot be viewed without authorization, but they ignore a minor privacy problem that arises when a user challenges the cloud server to seek data sharing from other users. Regardless of whether the contested access request is granted data access rights, it may disclose the user's privacy. In this research, we propose a shared authority-based privacy-preserving authentication protocol (SAPA) to solve the aforementioned privacy concerns for cloud storage. Within the SAPA,
JingiLi, Jinet al. presents a design to handle the challenge of integrity audits and safe deduplication on cloud data. Specifically, two secure systems, Sec Cloud and Sec Cloud+, are proposed with the goal of ensuring both data integrity and deduplication in the cloud.Sec Cloud offers an auditing entity with the maintenance of a Map Reduce cloud, which assists customers in generating data tags prior to uploading as well as evaluating the integrity of data kept in the cloud.
Prof. Rucha R. Galgali investigated the problem related to the data privacy variousschemes are proposed based on the attribute based encryption techniques, still more attention is on privacy of the data content and the access control of the data and less attention is on the privilege control and the privacy of user's identity. These offer the Anony Control system, which addresses both data privacy and user identity privacy. They also provide Anony Control-F, which totally prevents identity difficulties. In the proposed concept, user revocation is included to allow for the activation and deactivation of users, increasing system efficiency and practicality.
F. Zhao et al. presented privacy-preserving authenticated access control in the cloud. Here, the researcher analyzes a centralized system in which a single key distribution center (KDC) distributes characteristics and secret keys to all users. However, a single key distribution center is not a single point of failure, and it is very difficult to sustain a large number of users on clouds.
H.K. Maji et al. established the ABS technique to enable anonymous user authentication, however it was a centralized approach.
K. Maji et al. offered a decentralized way to authentication that does not reveal the user's identity, although it is vulnerable to replay attacks.
A. Sahai and B. Waters introduced Fuzzy Identity-Based Encryption, which comprises of a single completely trusted centralized authority (CA) and many attribute authorities. Each user is assigned a unique global identifier, and the keys from different authorities are bound together by this identifier. To counteract a collusion attack, multiple users can pool their secret keys obtained from different authorities in order to decrypt ciphertext to which they are not individually entitled.
Kan Yang et al. suggested A decentralized architecture and strategy do not provide assurance to consumers that need anonymity while utilizing the cloud. However, the technique failed to offer user verification.
S. Ruj et al. presented a distributed access control module for clouds. In this strategy, user verification was not available. The second flaw was that users may create and keep a record while other users could just view it. Users other than the creator did not have write access.

4. Methodology

Cloud-stored data is protected by a distributed access control system, which allows access to the data only by authorized users with legitimate credentials. User authentication is used for cloud data storage and modification. During the authentication process, the cloud protects the user's identity. Because of the cloud's decentralized nature, many KDCs may handle key management. Collusion resistance is a feature of both authentication and access control systems. Because of the collusion-resistant attack, even if two users are not individually allowed, they cannot band together to authenticate themselves or access data. Once their account has been canceled, users are no longer able to access data. Replay attacks may be accommodated by the suggested protocol. The data saved in the cloud may also be accessed and written to several times using this suggested protocol. Decentralized techniques ought to be less expensive than the current centralized ones.

Figure 1: Architecture of Cloud

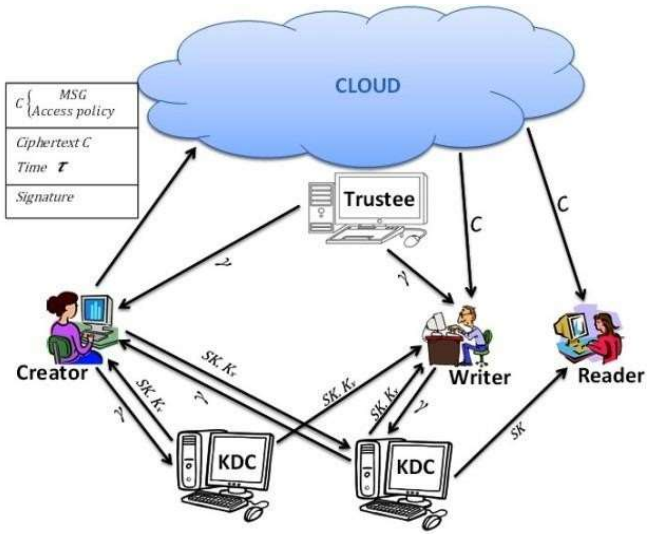

Fig. 1 show the suggested system's architecture. A writer, a reader, and a maker are the three users. The trustee gives a token to creator Alice, who is presumed to be honest. A trustee may be the federal government, which is in charge of social insurance numbers and other records. The trustee provides her a token once she shows her identification, social insurance number, health information, etc. There are many KDCs that may be dispersed. These KDCs may be servers located all over the globe. When a creator presents the token that was obtained from the trustee to one or more KDCs, they are given keys for encryption, decryption, and signature. Secret keys (SK) for decryption are provided in Figure 1; the keys are Kx for signature. The MSG message is encrypted under access policy X. Who has access to the data kept in the clouds is determined

by the access rules. The author chooses to demonstrate her signature and the message's legitimacy on a claim policy Y. The signed ciphertext C is sent to the cloud. The encrypted text (C) is stored in the cloud by confirming the signature.The cloud transmits ciphertext C to the reader if they choose to read the data. If the user has a set of characteristics that fit the access policy, the cipher text C may be decoded and the original message can be recovered.

5. Analysis & Result

5.1 Attribute-Based Encryption

The attributebased encryption concept was first proposed by A. Sahai and B. Waters[14]. ABE is a type of public-key encryptionis in which the ciphertext andsecret key of a user are dependent upon attributes. A crucial security feature of ABE is collusion resistance, an opponent holds multiple keys should alone be able to access data and information if at least single individual key grants access.In ABE the ciphertext decryption is possible only if the valid set attributes of the user key matching the attributes of the ciphertext.The ABE consists of four algorithms as follows

- System Initialization

Select a prime q, generator g of G0, groups G0 and GT of order q, a map e : G0X G0→ GT , and a hash function H :

{0,1}*→G0 that maps the identities of users to G0. The hash function used here is SHA-1. Each KDC Aj ϵ A has aset of attributes Lj. Each KDC also chooses two random exponents.

Key Generation and Distribution

User Uu receives a set of attributes I[j,u] from KDC Aj, and corresponding secret key SKi,u for each iϵI[j,u]. Where αi,yiϵSK[j]. Note that all keys are delivered to the user securely using the user's public key, such that only that user can decrypt it using its secret key.

- Encryption

In the encryption function by using the method ABE the message MSG is encrypted with the access policy X and the encrypted message which isciphertext C is sent.

- Decryption

In the decryption function the ciphertext C is decrypted by using the secret key SK to obtain the original message MSG.

5.2 CP-ABE System

A decentralized CP-ABE system is composed primarily of a set of A authorities, a trusted initializer and users. The only responsibility of trusted initializer is generation of system global public parameters that are system wide public parameters available to each entity in the system. During system initialization, every authority Aj ϵ A controls a different set U j of attributes and issues corresponding secret attribute keys to users. It has been observed that each authorities can work independent. As such, each authority is totally unaware of the existence of the other authorities in the system. In the system every user is identified with a unique global identity ID ϵ {0,1} and allowed to request secret attribute keys from the various authorities. In the system at any point of time, every user with global identity ID possesses a set of secret attribute keys that reflects a set LID of attributes, that we call an attribute set of the user with identity ID. Let UAjϵAU j, where Uj1∩Uj2=ϕ, for j1≠j2 be the attribute universe of the system. As a result of lack of global coordination between authorities, different authorities might hold identical attribute string. To overcome this, we can treat every attribute as a tuple consisting of the attribute string and also the controlling authority identifier. The decentralized CP- ABE consists of five algorithms

System Initialization(k): Initially, according to the security parameter k a trusted initializer choses global public parameter GP. Any user or any authority in the system can make use of these GP in order to perform their executions. Authority Setup(GP, Uj): Once during initialization every authority Aj ϵ A runs this algorithm. It accepts global public parameter GP and a set of attributes U j as input and outputs public key PubAj and master secret key MkAj of the authority Aj.

Authority KeyGen(GP,ID,a,MkAj):On receiving a secret attribute key request from the user every authority executes this algorithm. It takes global public parameter GP, global ID of a user, attribute a hold by authority and the master secret key of the corresponding authority as input and it returns a secret attribute key SKa,ID for the identity ID. Encrypt(GP,M,A,{PubAj}):An encryptor runs this algorithm and takes global public parameter GP, an access structure, message M to be encrypted and public key of relevant authorities corresponding to all attributes as input. Then it encrypts message M under access structure and returns the CT ciphertext.

Decrypt(GP,CT,{SKa,ID|aϵLID}):Decryptor with identity ID runs this algorithm on receiving ciphertext CT by inputting GP, CT and {SKa,ID|aϵLID}. Then it outputs the message if the user attribute set LID satisfies the access structure, if not satisfies decryption fails.

6. Conclusion

This work introduces a mechanism known as decentralized access control technique with anonymous authentication, which prevents replay attacks and user revocation. The identity of the user storing data and information is unknown to the cloud; only user credentials are checked. The distribution of keys is decentralized, concealing the user's access policy and attributes. Furthermore, the performance of attribute-based encryption and decentralized attribute-based encryption can be contrasted.

References

1. Amol D Shelkar, Prof.Rucha R. Galgali, " Data Access Privilege With Attribute Based Encryption and User Revocation", International Research Journal of Engineering and Technology (IRJET), Nov 2016.

2. Praveen N.R and Renju Samuel," Enhanced Efficient User Revocation Mechanism on Top of Anonymous Attribute Based Encryption" , International Journal of Emerging Technology in Computer Science Electronics, AUGUST 2016.

3. M. Satishkumar,B. dayKumar,Ch.ArunKumar,"Attribute Based Data Sharing with At tribute Revocation to Control Cloud Data Access", International Journal of Computational Science, Mathematics and Engineering, February-2016.

4. Muhammad YasirShabir, AsifIqbal, ZahidMahammad, and AtaullahGhafoor, " Analysis of Classical Encryption Techniques in Cloud Computing" , ISSN 1007-0214 09/10 pp102-119 Vol. 21, Number1, February 2019.

5. E.J. Coyne, D.R. Kuhn and T.R. Weil, "Adding Attributes to Role-Based Access Control" IEEE Computer, vol. 43, no. 6, pp. 79-81,June 2010.

6. M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings" Proc. Sixth International ICST Conference Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.

7. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation" Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.

8. G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services" Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.

9. F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems" Proc. Seventh International Conference Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.

10. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th International ICST Conference Trust, Security and Privacy in Computing and Communications (TrustCom), 2011