International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Attribute Based Encryption Techniques of Cloud Computing Access Control

Deepali Madan Adhav[1], Mallikarjun M. Math[2]

[1]Student(M.Tech), Gogte Institute of Technology, Belagavi, Karnataka
[2]Professor, Gogte Institute of Technology, Belagavi, Karnataka

Abstract:
Cloud computing has emerged as a transformative development in the realm of Information Technology. The advent of services like "on-demand" and "pay-as-you-go" has led to the migration of both government and industrial IT infrastructures up in the clouds. With data and business logic being stored on remote cloud servers, the security concerns connecting to the cloud environment differ from those of traditional computing. In the domain inside cloud computing, data security is administered by Cloud Service Providers (CSPs), leaving owner of the data with limited control over the security policies governing their own data. Privacy and saftey stand out as two critical factors that discourage users from transitioning to untrusted cloud environments. Despite the substantial savings in costs associated with cloud adoption, ensuring secured data sharing consistently remains a top priority for data owners. As a result, these two aspects demand heightened attention to facilitate securely sharing data within the cloud computing landscape. This paper undertakes a comprehensive review and comparison of various attributebased encryption schemes within the context of cloud computing.

Keywords: Access control, Attribute-based encryption, Cloud computing, CP-ABE, CP-ASBE, HASBE, KP-ABE.

I. Introduction

Cloud computing use is rising quickly because of its many advantages. Cloud computing has evolved into a transformative force for organizations within the new IT architecture. Public, private, community, and hybrid clouds are the four primary cloud deployment modes as defined by the NIST framework, according to Badger et al. (2011) [2]. According to the Cisco Global Cloud Index research, by 2021, global traffic to cloud data centers is expected to reach 20.6 ZB annually [1].

The rise in popularity of cloud computing can be attributed to its features such as cost reduction, pay-per-usage, virtualization, on-demand access, multi-tenancy, and scalability. In this landscape, users and data owners store and share data with others. Consequently, cloud service providers have a responsibility to ensure trust and security for their users. As cloud users entrust sensitive and personal data to the cloud, the risk of data breaches by malicious intruders remains a significant concern.

Before data is uploaded to the cloud, encryption is crucial for preserving its security and private. Plain messages are converted into cipher messages through encryption, making them unintelligible to unauthorized parties. Although traditional public key infrastructure has been widely used for secure data sharing, real-time cloud applications and broadcasting data from the cloud are less effective with it.

Controlled access, in addition to encryption, is essential to cloud computing for maintaining the confidentiality, integrity, and availability of data. Access control is a key strategy for controlling who can access a system. Models of access control can be categorized as Discretionary, Mandatory, or Role-Based. Cloud computing is a good fit for role-based access control (RBAC) models because they adhere to the idea of giving users the least amount of permission possible depending on their responsibilities.

Large, distributed cloud environments have specific requirements, thus policy-based access control techniques were developed to suit these needs.

This study explores many attribute-based encryption strategies intended to control access to cloud data. Amit Sahai and Brent Waters were the ones who first proposed the idea of attributebased encryption (ABE) for safe data exchange in a cloud setting. ABE uses an access tree structure to work as a one-tomany encryption system [3]. It is a type of encryption with a public key where the ciphertext and secret key of the user are linked to particular properties.

II. Literature review

A. Attribute Based Encryption

Within the realm of cloud environments, various encryption schemes play a pivotal role in ensuring the security and confidentiality of data. One such encryption scheme is attributebased encryption (ABE), which was initially proposed by Sahai and Waters in 2005. ABE operates as a one-to-many encryption method, allowing data to be decrypted by multiple users.

By using the public key and master key, this system allows authorized users to decrypt ciphertext that matches certain criteria that they have in their possession. In order to enable encryption and decryption procedures, the key generation center assumes the position of an authority charged with generating keys for both data owners and consumers.

The key generation center receives requests from data users who meet certain criteria. The public key and master key are then combined by this authority to create a secret key for the data user. If the data user's qualities meet the relevant requirements, they can then utilize the acquired secret key to decrypt encrypted data. Even if attribute matching exceeds a certain threshold value, the data user's private key can still be used to decrypt encrypted data [4].

This system makes sure that only individuals with permission can access the data. However, this technique has a drawback in that in order to encrypt data, the data owner must also have access to each user's public key.

B. Encryption Using Key Policy Attributes

In 2006, Goyal et al. introduced KP-ABE [4], a scheme that associates an access policy, also known as an access structure, with the secret key or private key of data users [6]. These techniques were developed out of the necessity to regulate access to cloud data independently of Cloud Service Providers (CSPs).

In this method, the message is initially encrypted by the data owner by using a symmetric Data Encryption Key (DEK). The encrypted communication is then further encrypted using the master key, the public key, and a number of defining parameters. A data user's key must match the corresponding properties specified by the file's access structure in order to access a cloudbased file. The user can then decrypt the encrypted key and then decrypt the original message once they are satisfied. Consider encrypted data that has descriptive qualities like "Photos" and "Friends," as well as a data user's private key that has the access structure "Photos" and "(Friends" and "Family").

However, an inherent issue with this plan emerges: while a user's, a private key can decrypt all ciphertext that matches the access structure's attribute set, the encryptor lacks the ability to selectively choose who can decrypt the encrypted data.

C. Expressive Key Policy Attribute-Based Encryption Scheme

This is an optimized variant of KP-ABE, designed for enhanced efficiency. It introduces the capability to manage nonmonotonic access structures while maintaining a consistent ciphertext size. Non-monotonic access tree structures encompass access schemes that may incorporate negated attributes [3]. In 2007, Ostrovsky et al. presented an attributebased encryption system featuring a non-monotonic access structure. Unlike the previous KP-ABE scheme, which lacked negative attributes, this new approach shares a similar access structure with KP-ABE. It extends the Boolean formula to encompass NOT operations alongside AND and OR gates.

For instance, imagine a college housing two departments: Management and Computer Science. If the college aims to share student data with its teachers, a teacher's private key could possess an access structure like {Results Teacher}. However, if a specific teacher should not have access to the results of the Computer Science department, the access structure incorporates a NOT operation. Consequently, Teacher "A" from the Management department would possess a secret key structured as {Results ^ Teacher ^¬Computer Science}, thereby restricting access to the Computer Science results [7].

Nonetheless, a challenge arises with this scheme: explicitly indicating negated attributes within the ciphertext. In the example given, the inclusion of "NOT Computer Science" in the ciphertext clarifies its lack of relevance to the Computer Science department. However, explicitly including negative attributes for all aspects unrelated to the ciphertext introduces an overhead, particularly in cases where numerous applications are involved. For instance, if additional departments become part of the college, the secret key would need to incorporate "NOT Chemistry," "NOT Biology," "NOT Commerce," "NOT Sociology," and so on. This can lead to increased ciphertext complexity. Additionally, complications can arise when the data owner encrypts a message without awareness of certain attributes or when new attributes emerge after the creation of the ciphertext [3].

D. Encryption using a Cipher Text Policy AttributeBased Scheme

Developed by Bethencourt in 2007, this kind of attribute-based encryption (ABE) marks another advancement in the area. In this method, encrypted data is connected to an access policy, often known as an access structure. The user's private key simultaneously acquires a set of descriptive properties [5],[8]. Take the encrypted data access structure "Photos" (Friends) (Family) as an example. Access to the information is made possible by the presence of qualities like "Photos Friends" in a user's private key. With this configuration, the owner of the encrypted data or both can specify which keys can access the data..

Compared to Key-Policy ABE (KP-ABE), the advantage of Ciphertext-Policy ABE (CP-ABE) lies in its ability to let the encrypted data itself determine who can decrypt it. This characteristic has rendered this scheme practical within cloud computing environments. However, it maybe not as suitable for modern enterprise settings demanding greater policy flexibility. Additionally, CP-ABE proves while dealing with, is less effective compound and numerical attributes [9]. Addressing these shortcomings, Bobba et al. introduced the Cipher Text Policy Attribute-Set Based Encryption, which overcomes these limitations.

E. Cipher Text Policy Attribute-Set Based Encryption Scheme

CP-ASBE, also known as ASBE, represents an extended iteration of CP-ABE. This advanced scheme was initially introduced by Bobba et al. in 2007. In ASBE, user attributes are structured within a recursive set arrangement rather than being logically grouped as a single set. This recursive set structure places restrictions on users, not allowing them to combine attributes sourced from a singular set [9]. A notable feature of this scheme is its support for compound attributes and the assignment of multiple numerical values to a single attribute.

To handle compound attributes effectively, Bobba et al. proposed an attribute table within this scheme. In this configuration, each row functions as a distinct set, allowing multiple rows to be associated with a user. For instance, consider a teacher instructing various subjects; their issued key structure could appear as follows: {{Subject=312, Class=C12, Year=2017}, {Subject=315, Class=C13, Year=2018}}

An inherent strength of this scheme lies in its ability to thwart collusion attacks, ensuring that encrypted data retained by data users within the cloud remain confidential, even in scenarios where the credibility of the cloud service provider is questionable.

F. Hierarchical Attribute-Set Based Encryption Scheme

HASBE stands as an expansion upon ASBE, designed to manage the hierarchical structure of system users. This advanced scheme delivers adaptable and scalable access control within the realm of cloud computing. In 2011, Wang et al. [10] introduced a hierarchical attribute-based encryption scheme,

effectively merging the attributes of a Hierarchical IdentityBased Encryption scheme (HIBE) with those of a ciphertextpolicy attribute-based encryption scheme, thereby achieving intricate access control [11]. HASBE encompasses a wide array of functionalities, including hierarchical user assignment, data file access, creation and deletion, as well as user revocation.

This system operates based on keys generated through HIBE's hierarchical key generation property. Its components encompass a trusted or root authority, multiple domain authorities, a multitude of data users, and data owners. The data owner's role entails storing encrypted data through cloud storage services and subsequently sharing it with authorized users. Meanwhile, the root authority assumes the responsibilities of generating system parameters, root master keys, and domain keys. These keys are then disseminated to upper-level domain authorities, with their authorization ensured by the root authority. The domain authority is tasked with managing its subsequent domain and all users within it. This includes delegating keys to domains at lower or subordinate levels and distributing secret keys to users within the domain. Users, in turn, utilize their secret keys to decrypt encrypted data and access messages, but only if the attributes associated with their key structures satisfy the cipher text policy [12]. Importantly, the key generation process adheres to a hierarchical approach.

Through the implementation of a comprehensive delegation algorithm, this scheme effectively achieves fine-grained access control over cloud resources. It even incorporates proxy reencryption capabilities. Nevertheless, practical implementation proves challenging, as attributes within a single conjunctive clause within this scheme may be under the purview of the same domain authority, while the same attribute could potentially fall within the control of multiple domain authorities.

III. comparIson anaLysIs

Having examined the aforementioned ABE schemes, this section aims to conduct a comparative analysis of these schemes using various criteria or parameters. The objective is to discern the most suitable ABE scheme for deployment within the cloud environment.

A. User Accountability

In cases where a deceitful authorized user shares their attribute secret key with an unauthorized individual, the potential for unauthorized access emerges. ABE and KP-ABE algorithms are susceptible to this issue, lacking the ability to ensure user accountability and prevent illicit access to encrypted data through attribute secret key sharing. In contrast, CP-ABE, CPASBE, and HASBE offer a solution by establishing user accountability. This is achieved through the association of the access policy with encrypted data, thereby mitigating the risk of unauthorized access.

B. Data Confidentiality

Encryption or re-encryption serves as a crucial measure to uphold data confidentiality and protect against unauthorized access, both from external sources and within the cloud environment itself. All of the aforementioned schemes successfully meet this criterion.

C. Fine Grained Access Control

Distinct access rights are allocated to each user, even within the same group. This unique attribute ensures that all encryption algorithms offer fine-grained access control. Notably, all schemes, with the exception of ABE, fulfill this criterion.

D. User Revocation

It is necessary to remove a user's access permissions when they are no longer a part of the system. By revoking access rights, the former user's ability to access data is effectively nullified.

Notably, CP-ABE, CP-ASBE, and HASBE offer robust mechanisms for user revocation, including the incorporation of attributes such as expiration times into a user's key structure.

E. Collusion Resistant

This criterion emphasizes the prevention of attribute combination among users to decrypt encrypted data. The design ensures that collusion among users is averted, with each attribute being linked to either

a polynomial or a random number. It is noteworthy that all the encryption algorithms examined in this context demonstrate resistance to collusion. Consequently, each of the discussed schemes satisfies this criterion.

F. Scalability

The efficacy of an algorithm should remain unaffected by an increase in the number of users. Remarkably, only HASBE adheres to the scalability criteria, achieved through the utilization of a full delegation algorithm.

G. Computation Overhead

Computational overhead is notably reduced through algorithmic enhancements from ABE to HASBE. Consequently, when juxtaposed with previous ABE encryption algorithms, the HASBE algorithm boasts the least computational overhead.

H. Access Structure

ABE, KP-ABE, and CP-ABE exhibit monotonic access structures, while EKP-ABE features a non-monotonic access structure, CP-ASBE employs a monolithic access structure, and HASBE employs a hierarchical access structure.

It is noteworthy that certain schemes may not fully meet the criteria of scalability and user accountability. However, all of these schemes successfully accomplish data confidentiality and collusion resolution. The ABE scheme, for instance, fulfills fundamental security requirements by satisfying two criteria. It utilizes attributes in a user's private key to align with attributes present in encrypted data. This foundational concept underpins various attribute-based encryption schemes. Notably, among the schemes discussed, only HASBE successfully meets all the established criteria while minimizing computational overhead.

Nonetheless, the criterion of user accountability poses challenges since the complex nature of resolving illegal keysharing issues among users. The result is, some ABE schemes we've explored may fall short in achieving two specific criteria: user accountability and scalability.

Iv. Conclusion and Future scope

Security policies and access control form a pivotal and sensitive domain for cloud vendors. Upon user authentication and access to the cloud, the user gains substantial freedom, enabling them to inadvertently or intentionally disrupt the cloud environment and trigger chaos. Cloud providers employ diverse technologies to furnish their users with fine-grained access control.

This paper delves into a comprehensive discussion and comparison of distinct attribute-based encryption schemes that facilitate fine-grained access control. We have analyzed and juxtaposed multiple schemes, including KP-ABE, CP-ABE, CP-ASBE, and HASBE, across various criteria. Flexible and scalable access control is required due to the complex structure of a large-scale distributed system like the cloud. Our goal in this research is to analyze the workings and procedures of various attribute-based encryption systems while also addressing the inherent flaws in them.

This paper's main contribution is its thorough examination and comprehension of the variety of attribute-based encryption techniques used in the context of cloud computing.

References

1. https://www.cisco.com
2. K. K. Hausman, S. L. Cook, and T. Sampaio, Cloud Essentials: CompTIA Authorized Courseware for Exam CLO-001, June 2013.
3. R. Ostrovsky, A. Sahai, and B. Waters, “Attribute based encryption with non-monotonic access structures,” In Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 195-203, 2007.

4. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," In Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), ACM, New York, USA, pp. 89-98, 2006.
5. L. Cheung, and C. Newport, "Provably secure ciphertext policy ABE," In Proceedings of the 14th ACM Conference on Computer and Communications
6. Security, ACM, p. 465, 2007.
7. C. Wang, and J. Luo, "An efficient key-policy attributebased encryption scheme with constant ciphertext length," Mathematical Problems in Engineering, vol. 2013, Article ID 810969, 2013.
8. C. C. Lee, P. S. Chung, and M. S. Hwang, "A Survey on attribute-based encryption schemes of access control in cloud environments," International Journal of Network Security, vol. 15, no. 4, pp. 231-240, July 2013.
9. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertextpolicy attribute-based encryption," In Proceedings of IEEE Symposium on Security and Privacy, pp. 321-334, 2007.
10. R. Bobba, H. Khurana, and M. Prabhakaran, "Attributessets: A practically motivated enhancement to attributebased encryption," In M. Backes, and P. Ning, (eds.), ESCORICS 2009, LNCS, pp. 587-604, 2009.
11. G. Wang, Q. Liu, and J. Wu, "Hierachical attribute based encryption for fine-grained access control in cloud storage services," In Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 735-737, 2010.
12. G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," Computer & Security, vol. 30, no. 5, pp. 320-331, 2011.
13. Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743-754, 2012.