ZKG INTERNATIONAL

ISSN: 2366-1313

ENHANCING CLOUD DATA SECURITY: ATTRIBUTE-BASED ACCESS CONTROL IN DECENTRALIZED CLOUDS

[#1]KOVIDA ARRAM,
[#2]ALUMALLA VEERA REDDY,
[#3]P.SRAVAN KUMAR, *Assistant Professor,*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Granular access control is required for data hosted on unreliable websites, such as cloud infrastructures. Because of the increased volume of data that must be managed, decentralized key management outperforms centralized key management. Encrypting and decrypting data on devices with limited resources can be both costly and inefficient. An ABE autonomous system has been designed, including remote decryption, quick encryption, and the ability to remove users. Because of its dependency on cloud storage for encrypted data and partial decryption of cipher texts, our solution was designed with the mobile cloud environment in mind. Mobile users can easily and affordably upload and download data from the cloud for encryption and decryption. The approach is divided into two stages: offline pre-processing and online encryption. Once the policy has been implemented, the device connects to the internet. When a device is not in use, it becomes inactive. Compared to the already established autonomous Attribute-Based Encryption (ABE) approaches, this approach is faster and more efficient. Consumers of data must generate a new iteration of the decryption key to avoid an untrustworthy proxy server from partially deciphering the encrypted content while limiting access to the original message. Once a part of the encrypted text has been decrypted, users can decode the full document without completing costly coupling operations. Furthermore, we offer the ability to unregister users from our system at no additional charge for online services. Compared to other ABE schemes, ours considerably reduces processing times for data owners and users. As a result, it works best on mobile devices.

Keywords:Encryption, Cloud computing, Servers, Performance evaluation, Access control

1. INTRODUCTION

Consider a common scenario in which data owners opt to store their data on unreliable servers, such as cloud storage, in order to secure its security in the future. Cell phones, wireless devices, and smartcards can store a large amount of data despite their limited storage capacity. The goal is to ensure that the data is long-term safe and available to as many people as possible. Individuals and businesses increasingly rely on cloud service providers (CSPs) to store their data. The majority of the reason for this is that customers believe these companies provide unlimited storage. Unfortunately, the negative image of cloud service providers (CSPs) causes many data owners to distrust them. This demand necessitates the implementation of safeguards for all cloud-based data. Data owners can put up access restrictions to guarantee that only authorized users can view their information. Hospitals may soon be allowed to transfer clinical study data—which examines the efficacy of new cancer medications—to the cloud. Only physicians and researchers working on new drugs have access to this highly private information. Data encryption could be achieved via attribute-based encryption (ABE). Authorities are dispersed or many. One of the primary benefits of attribute-based encryption (ABE) systems is that they do not rely on a single

ISSN: 2366-1313

authority to create and distribute decryption keys for diverse qualities. A medical researcher may acquire a patient's medical records from a study organization rather than from the hospital. User attributes may change frequently owing to changes in location, work, and other variables. Someone who used to have access to data may not have the necessary credentials anymore. Even if the user's characteristics change, they can still view the data. Users rejecting them is thus critical for ABEs. Using such sophisticated encryption mechanisms further complicates issues. On a system with limited resources, it is hard to decode or produce revocation keys quickly enough. Decentralized attribute-based encryption (ABE) enables users to quickly safeguard data, remove permissions, and decode data from the outside, effectively resolving this issue. Users of mobile devices can share and download encrypted data from DropBox without having to pay a lot of money to encrypt and decrypt it because the mobile cloud has limited storage capacity and only partially decrypts data. To avoid the prohibitively high cost, the most expensive encryption algorithms are used offline. This is done to cover the times when the gadget is charging, not in use, or the encryption procedure takes longer than expected. When connected to the internet, the device can only perform a few computations at once. Users can so continue to work undisturbed.

Data owners save time and effort by not having to undertake decryption methods themselves. Because the proxy server has its own unique decrypting key, it can partially decrypt protected data. However, partial decryption cannot be used to improve a weak proxy service. To decrypt the cipher text and get the final plaintext, take a few simple procedures. Similar to revocation keys, these keys can be generated offline and then delivered to the proxy server after certain computations to alter the keys online. To lay the groundwork for our strategy, we'll look at these two case examples.

People are increasingly employing Wi-Fi-enabled sensor networks to collect data on the behavioral, mental, and physical aspects of the aged. Encryption is required to ensure that this information remains secure for future use. Scholars and caregivers may find this material useful in understanding environmental factors, illnesses, the aging process, early detection, and intervention. To collect data, researchers may need to get the necessary categories from non-hospital populations. When multiple companies have access to the same data, they can collaborate effectively. When using services such as Drop Box, team members can submit work from their phones while traveling. To ensure security, critical data, such as banking information and trade secrets, must be encrypted before uploading. Everyone involved in the project has access to this information. Nonetheless, group members have various alternatives for highlighting their contributions to a project on their résumés.

2. LITERATURE REVIEW:

The rising use of cloud access control is due to the importance of ensuring that only authorized users have access. The cloud stores vast amounts of data, including sensitive information. Attribute-Based Encryption (ABE) is a cryptographic technology that uses a variety of decryption methods to encrypt data on the cloud. To help clients make informed purchasing selections, a thorough list of qualities and their accompanying criteria is provided. Only clients that are anatomically identical to those used for data storage in the cloud can decrypt data. According to my research, there are a number of reasons why people may be unable to access medical care. They use cloud-based verified access control to protect privacy. A centralized key distribution center (KDC) continues to send client data and confidential keys. Real-world management of a single Key Distribution Center (KDC) is difficult due to the large number of KDCs that require supervision and administration. This

ISSN: 2366-1313

approach does not support authentication using symmetric keys. The primary emphasis of the study was multi-authority attribute-based encryption (ABE), a technology that eliminated the need for a trusted authority to verify that each client possessed characteristics from each key distribution center (KDC). Currently, centralized access control in cloud computing is the norm. Attribute-based encryption (ABE) is commonly implemented using only two methods. Despite using symmetric key schemes, these methods are unsuitable for authentication. These procedures are unsuitable for authenticating needs. Zhao et al. have created a mechanism for authenticating cloud access while maintaining confidentiality. Key distribution centers, or KDCs, allow access to private keys and other features. The existence of a high number of users in a cloud environment can hamper the operation of a single Key Distribution Center. We underline the importance of decentralizing the distribution of cloud user attributes and secret keys as a result. Many Key Distribution Centers (KDCs) are distributed around the world and serve as vital infrastructure for cloud computing. Waters and Sahai conceived ABE. In attribute-based encryption, an individual's unique identifier is one of numerous differentiating features. There are two different types of ABEs. Goyal and his colleagues devised the shorter abbreviation "KP-ABE," which stands for "key-policy ABE." Because of the restricted access, the person who transmitted the information can keep it secure. Regaining access to the system after misplacing or having their logon credentials and set of keys stolen is a difficult chore for the author. The receiver must use their confidential keys and recipient attributes to decode the data. The recipient uses a tree-like access policy, with characteristics serving as the leaves; the cipher ext-policy includes the operators AND, OR, and CP-ABE. The Key Distribution Center (KDC) is vulnerable because of its central location and has a single point of failure. According to Chase's assessment, certain Key Distribution Centers (KDCs) issue private and unique keys to individuals. Maji et al.'s ABSs support anonymous user login. As a result, a specified level of centralization was chosen. Maji et al. claim that their system takes a decentralized approach while also protecting consumers' privacy. People often try to strike it many times.

3. PROPOSED SYSTEM:

We propose a fast-encrypting and decrypting CPABE device. Entry control is decentralized since the system is outsourced to a third party. Our technique dramatically cuts computational costs in a decentralized system for both consumers and data owners. Costs have never been reduced in this way before. The CPABE scheme's decentralized structure, online/offline encryption mode, and outsourcing decoding capacity enable its use in the real world. We base our approach on Lewko and Waters' proposal for Decentralized CPABE. Currently, we have:

1) Fast Online/Offline Encryption: The most expensive computations in the age of internet encryption involve only multiplication.

2) Outsourced Decryption: Data can be decrypted halfway using the encrypted secret keys provided by the data user to the proxy server. In this case, there are no bilinear pairs to complete; the individual decrypting the data only needs to do a predefined number of exponentions. Because the data is not decrypted by a central authority, our technique operates autonomously and does not require assistance from one.

3) Security and performance: Our methodology has been demonstrated to be safe, as the Lewko-Waters method is thought to be safe for prime order groups. We support this assumption with genuine mathematical reasoning rather than sketch proofs. The previous version made it impossible to create and implement an online offline multi-authority CPABE scheme without external decryption.

ISSN: 2366-1313

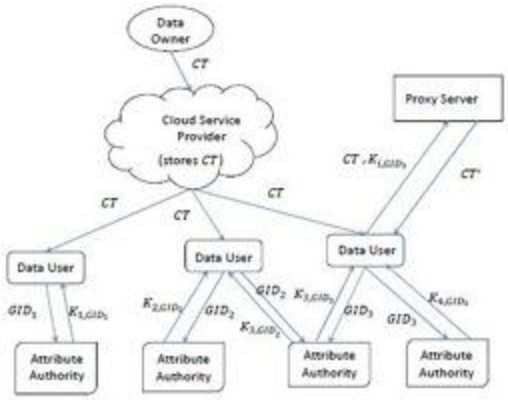

Fig1: System Architecture

4. EXPERIMENTAL RESULTS:

5. COMPARATIVE STUDY

ISSN: 2366-1313

Scheme	Access Control Yes=Y, No=N	Decentralized / Centralized	Read/ Write	Type of Access control	Authentication	Client Revocation
[12]	Y	Centralized	1-W-M-R	Symmetric Key Cryptography	No Authentication	No
[9]	Y	Centralized	1-W-M-R	ABE	No Authentication	No
[15]	Y	Decentralized	1-W-M-R	ABE	No Authentication	Yes
[14]	Y	Decentralized	1-W-M-R	ABE	Not Privacy Preserving	Yes
[11]	Y	Centralized	M-W-M-R	ABE	Authentication	No
[1]	Y	Decentralized	M-W-M-R	ABE	Authentication	Yes
Our scheme	Y	Decentralized	M-W-M-R	KDC (Access Policy), sABE	Authentication	Yes

6. CONCLUSION:

As evidenced by the approach's random oracle proof, we created a CPABE scheme with a prime ordering. Prime order groups are employed because they are effective and speed up group activity. Using complex security ideas, we are able to create a Composite order group scheme that is ineffective in the dual system encryption model. That is something that must be completed later. A multi-authority online-offline system or framework enables multiple authorities or entities to operate simultaneously online and offline. CPABE was commissioned to handle the encryption. Various authorities, both online and offline CPABE stands for Ciphertext Policy Attribute-Based Encryption. Unfortunately, the user is unable to identify whether the partial decoding was successful. This publication may be useful in solving the following problems. Using a similar strategy, we may tackle our confirmed outsourcing issue. One proposed solution was to hire people who could be checked. Our plan is unique and honest, thus we do not wish to reveal it. More research is needed to disprove this opinion about outsourcing demonstrated decryptions. We cannot solve it. This paper proposes Attribute-Based Encryption (ABE) for mobile clouds. The system allows for the removal of users, offers rapid encryption, decoding outsourcing, and is decentralized. Because all computations requiring significant processing power are performed offline, the encryption method in this system is faster and more efficient than in previous decentralized Attribute-Based Encryption (ABE) systems. However, because they do not have access to the original, unencrypted data, proxy sites you cannot trust can only decrypt a small fraction of the encrypted data. Users of data can decipher partially encrypted content without paying for costly pairing processes. Users can cancel their orders online for free using our system. Unlike earlier systems, our technique strikes a reasonable balance between encryption and decoding rates and allows users and data to be erased and retained separately.

REFERENCES

1. Sushmita Ruj, Member, IEEE, Milos Stojmenovic, Member, IEEE, and Amiya Nayak, Senior Member, “Decentralized Access Control with AnonymousAuthentication of Data Stored in Clouds” IEEE,2014.
2. Ajith Singh. N, Department of computer science, Karpagam University, Coimbatore, India, M. Hemalatha, Department of software systems & research, Karpagam University, Coimbatore, India, “Cloud computing for Academic Environment”.
3. Luit Infotech Private Limited, Bangalore, India, “Luit Infotech SaaS Business Software”.
4. Wang, Q.Wang, K.Ren, N.Cao and W.Lou, “Toward Secure and Dependable Storage Services in Cloud Computing”, IEEE Services Computing, Vol. 5, no.2, pp. 220-232, 2012.
5. C. Gentry, “A fully homomorphic encryption scheme”, Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.
6. Yang Tang, Patrick P.C. Lee, John C.S. Lu and Radia Perlman, “Secure Overlay Cloud Storage with Access Control and Assured Deletion”, IEEE Transactions on dependable and secure
7. R. Perlman, “File System Design with Assured Delete,” Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007

ISSN: 2366-1313

8. Rahumed, H.C.H. Chen, Y. Tang, P.P.C. Lee, and J.C.S. Li,"A Secure Cloud Backup System with Assured Deletion and Version Control," Proc. Third Int'l Workshop Security in Cloud Computing, 2011
9. Personal M. Li, S. Yu, K. Ren, and W. Lou, "Securing health records in cloud computing: Patient-centric and fine-grained data access control in multi owner settings," in SecureComm, pp. 89–106, 2010.
10. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ACM ASIACCS, pp. 261–270, 2010.