ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Efficient Implementation of Cipher Text-Policy Attribute-Based Encryption (CP-ABE) Dependent Access Control Scheme for Multi-Authority Cloud Storage Systems

Konu Anusha
M.Tech Student
Department of CSE
Audisankara Institute of Technology,
Gudur.

Vadlapudi Mamatha
Associate Professor
Department of CSE
Audisankara Institute of Technology,
Gudur.

ABSTRACT:

Controls on data in the cloud computing environment include the governance policies set in place to make sure that your data can be trusted. The integrity, reliability, and confidentiality of your data must be beyond reproach. And this holds for cloud providers too. :In a Cloud Computing the data security achieved by Data Access Control Scheme. Cipher text-Policy Attribute-based Encryption (CP-ABE) is considered as one of the most suitable scheme for data access control in cloud storage. This scheme provides data owners more direct control on access policies. However, CP-ABE schemes to data access control for cloud storage systems are difficult because of the attribute revocation problem. In this paper we study and implement a revocable multi-authority CP-ABE scheme. The attribute revocation method can efficiently achieve both forward security and backward security. This survey shows that revocable multi-authority CP-ABE scheme is secure in the random oracle model and is more efficient than previous multi-authority CP-ABE.

Keywords: ***CP-ABE, Data Control, Cloud Computing, Access control, Multiple Authority***

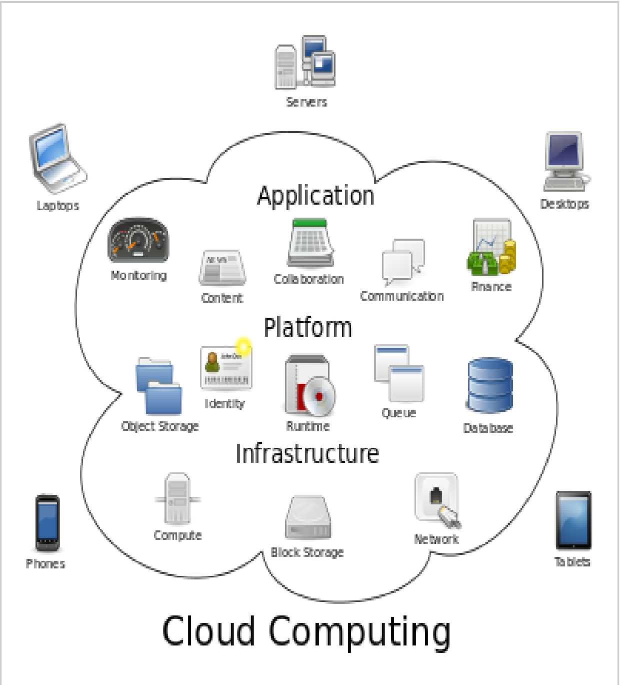
Introduction:

Cloud computing allows application software to be operated using internet-enabled devices. Clouds can be classified as public, private, and hybrid. Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

The term "moving to cloud" also refers to an organization moving away from a traditional CAPEX model (buy the dedicated hardware and depreciate it over a period of time) to the OPEX model (use a shared cloud infrastructure and pay as one uses it).

Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing have led to a growth in cloud computing. Companies can scale up as computing needs increase and then scale down again as demands decrease.



Cloud computing metaphor: For a user, the network elements representing the provider-rendered services are invisible, as if obscured by a cloud.

Cloud computing exhibits the following key characteristics:

Agility improves with users' ability to re-provision technological infrastructure resources.

Cost reductions claimed by cloud providers. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state-of-the-art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

Device and location independence enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

Performance is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.

Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.

Security and Privacy:

Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies which users have to agree to before they start using cloud services.

Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access.
According to the Cloud Security Alliance, the top three threats in the cloud are "Insecure Interfaces and API's", "Data Loss & Leakage", and "Hardware Failure" which accounted for 29%, 25% and 10% of all cloud security outages respectively — together these form shared technology vulnerabilities. In a cloud provider platform being shared by different users there may be a possibility that information belonging to different customers resides on same data server. Therefore Information leakage may arise by mistake when information for one customer is given to other. Additionally, Eugene Schultz, chief technology officer at Emagined Security, said that hackers are spending substantial time and effort looking for ways to penetrate the cloud. "There are some real Achilles' heels in the cloud infrastructure that are making big holes for the bad guys to get into". Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack — a process he called "hyperjacking".

Access Control in Cloud Computing:

Cloud computing is one of the emerging technologies. The cloud computing contains huge open distributed system. It is important to protect the data and privacy of users. Access Control methods ensure that authorized users access the data and the system. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security.

Cloud Storage:

The Cloud storage is an important service of cloud computing. The Cloud Storage offers services for data owners to host their data into the cloud. A great challenge to data access control scheme was data hosting and data access services. Because data owners does not fully trust the cloud servers also they can no longer rely on servers to do access control The data access control becomes a challenging issue in cloud storage systems because of data outsourcing and untrusted cloud servers. Therefore Cloud storage is a model of data storage where the digital data is stored in logical pool.

CP-ABE:

One of the most suitable technologies for data access control in cloud storage systems is Cipher text-Policy Attribute-based Encryption (CP-ABE). This scheme provides the data owner more direct control on access policies. The Authority in CP-ABE scheme is responsible for attribute management and key distribution. The authority may be the university registration office, the human resource department in a company, etc. The data owner in CP-ABE scheme defines the access policies and encrypts data according to the policies.

CP-ABE TYPES:

In CP-ABE scheme each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the access policies.
There are two types of CP-ABE systems:

1. Single-authority CP-ABE
2. Multi-authority CP-ABE

In Single-authority CP-ABE scheme, where all attributes are managed by a single authority. In a Multi-authority CP-ABE scheme where attributes are from different domains and managed by different authorities. This method is more appropriate for data access control of cloud storage systems. Users contain attributes those should be issued by multiple authorities and data owners. Users may also share the data using access policy defined over attributes from different authorities.

Data Access Control System In Multi Authority Cloud Storage

There are five types of entities in the system AS IN Fig 1: a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users). The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system.

For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity. Every AA is an independent attribute authority that is responsible for entitling and revoking user‟s attributes according to their role or identity in its domain.

EXISTING SYSTEM:

This new paradigm of data hosting and data access services introduces a great challenge to dataaccess control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitabletechnologies for data access control in cloud storage systems,because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution.

DISADVANTAGES OF EXISTING SYSTEM:

- Chase’s multi-authority CP-ABE protocol allows the central authority to decrypt allthe ciphertexts, since it holds the master key of the system.
- Chase’s protocol does not support sattribute revocation.

PROPOSED SYSTEM:

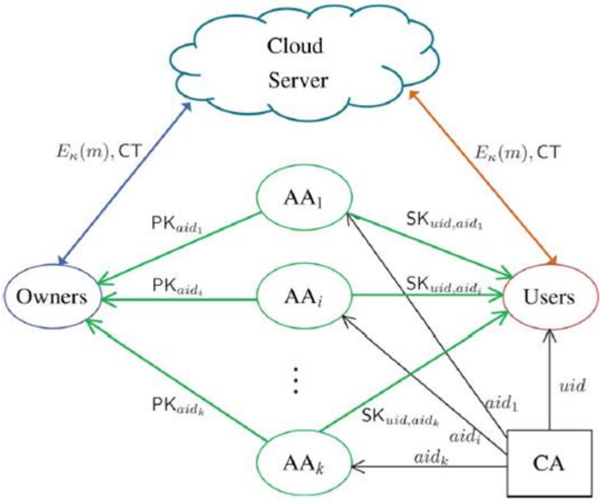
In this paper, we first propose a revocable multiauthority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system.

Our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt)and forward security (The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficient.attributes). Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semitrusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

ADVANTAGES OF PROPOSED SYSTEM:

- We modify the framework of the scheme and make it more practical to cloud storage systems, in which data owners are not involved in the key generation.
- We greatly improve the efficiency of the attribute revocation method.
- We also highly improve the expressiveness of our access control scheme, where we remove the limitation that each attribute can only appear at most once in a ciphertext.

SYSTEM ARCHITECTURE:



Conclusion:

This paper examines and implements a revocable multi-authority CP-ABE scheme that can support efficient attribute revocation. Then the effective data access control scheme for multi-authority cloud storage systems is proposed. It eliminates Decryption overhead for users according to attributes .This secure attribute based cryptographic technique for robust data security that‟s being shared in the cloud .This revocable multi-authority CPABE scheme with Verifiable outsourced decryption and proved that it is secure and verifiable .The revocable multi-authority CPABE is a efficient technique, which can be applied in any remote storage systems and online social networks etc.

References:

[1] Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE“Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,VOL. 25,NO. 7,JULY 2014.

[2]. J. Hur and D.K. Noh, „„„Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,“““ IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[3].S.Jahid, P.Mittal, and N.Borisov, „„„Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,“““ in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS‟11), 2011, pp. 411-415.

[4].M. Li, S. Yu, Y. Zheng, K. Ren, andW.Lou, „„„Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,“““ IEEE Trans. Parallel Distributed Systems, vol. no. 1, pp. 131-143,Jan. 2013. 24,

[5].Kan Yang, and Xiaohua Jia,Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage,“““ IEEE transactions on parallel and distributed systems, vol. 25, no. 7, july 2014.

[6] MrSanthoshkumarB.J, M.Tech, Amrita VishwaVidyapeetham, Mysore Campus, India “Attribute Based Encryption with Verifiable Outsourced Decryption.” In International Journal of Advanced Research in Computer Science and Software Engineering”Volume 4, Issue 6, June 2014,ISSN: 2277 128X.

[7]Tejaswini R M1, Roopa C K2 , Ayesha Taranum “Securing Cloud Server & Data Access withMulti-Authorities” International Journal of Computer Science and Information Technology Research ISSN 2348-120X Vol. 2, Issue 2, pp: (297-302), Month: April-June 2014,

[8] www.ijracse.com

[9] C. Dong, G. Russello, and N. Dulay, “Shared and Searchable Encrypted Data for Untrusted Servers,” J. Computer Security, vol. 19, pp. 367- 397, 2010.

10. D. Boneh and M.K. Franklin, Identity-Based Encryption from the Weil Pairing,“““ in Proc. 21st Ann. Int’l Cryptology Conf.: Advances in Cryptology - CRYPTO’01, 2001, pp. 213-229.