International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-10 E-ISSN: 2347-2693

Manage Cloud Data Access Control Anonymity with Attributed Based Encryption

Thirumanapally Prashanth[1*], Gundu Purna Chandar Rao[2]

[1]Dept. of CSE, Hasvita Institute of Science and Technology, R.R District, India
[2]Dept. of CSE, Osmania University, Hyderabad, India

**Corresponding Author: prashanth.thirumanpally@gmail.com*

Available online at: www.ijcseonline.org

Received: 19/Sep/2017, Revised: 03/Oct/2017, Accepted: 18/Oct/2017, Published: 30/Oct/2017

***Abstract*—** Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been to secure the cloud storage. Data content privacy. A semi anonymous privilege control scheme AnonyControl to address not only the data privacy. But also the user identity privacy. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. The Anonymity –F which fully prevent the identity leakage and achieve the full anonymity.

Keywords— Cloud Computing, Anonymity, Multi Authority, Attribute-Based Encryption.

I.INTRODUCTION

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a „cloud". It greatly attracts attention and interest from both academia and industry due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the best of our knowledge. First of all, data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control. More likely, users want to control the privileges of data manipulation over other users or cloud servers. This is because when sensitive information or computation is outsourced to the cloud servers or another user, which is out of users" control in most cases, privacy risks would rise dramatically because the servers might illegally inspect users" data and access sensitive information, or other users might be able to infer sensitive information from the outsourced computation. Therefore, not only the access but also the operation should be controlled. Secondly, personal information (defined by each user"s attributes set) is at risk because one"s identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client"s personal information.

Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers. Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir [1], in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it. Few years later, Fuzzy Identity-Based Encryption [2] is proposed, which is also known as Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter"s identity has some overlaps with the one specified in the ciphertext. Soon after, more general tree-based ABE schemes, Key-Policy Attribute-Based Encryption (KP-ABE) [3] and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [4], are presented to express more general condition than simple „overlap". They are counterparts to each other in the sense that the decision of encryption policy (who can or cannot decrypt the message) is made by different parties.

Existing System:
Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir, in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it. Few years later, Fuzzy Identity-Based Encryption is proposed, which is also known as Attribute-Based Encryption (ABE).

Disadvantages:
Privacy risks would rise drastically because the servers may illegally inspect user's data and access sensitive information. Personal data is at risk because one's identity is authenticated based on his/her data. Scope of collude(come to a secret understanding) with malicious Data Consumers or Data Owners to harvest others" file contents to gain illegal profits.

II. PROPOSED SYSTEM AND ARCHTICTURE

1: Policy Attribute-Based Encryption With Privacy Preserving In Clouds

To decentralize Access Control Scheme for secure data storage (ABE & ABS).In this scheme we only give the privacy to attribute based encryption. And attribute based scheme .In attribute based encryption scheme we use the Anonym control Scheme.

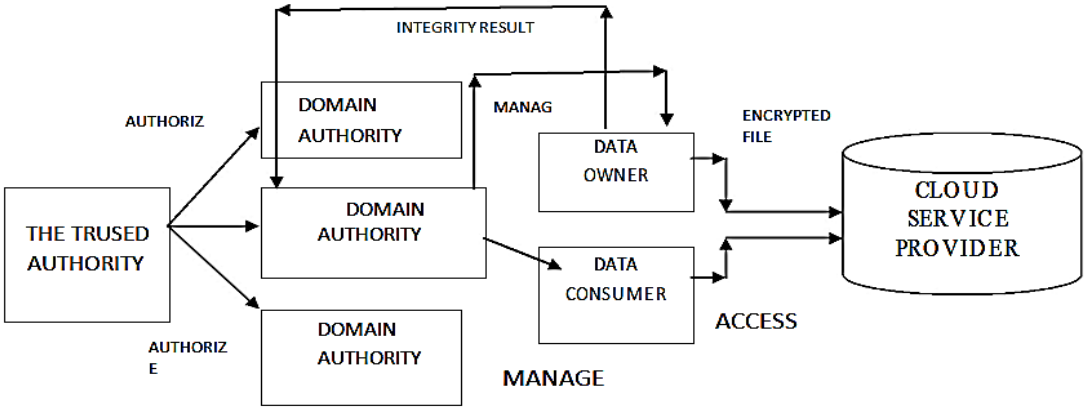

Fig: 1.Archticture System

2: Cipher text based policy attribute based encryption

As compared to existing schemes, our proposed solution enables the authority to revoke user attributes with minimal effort. We achieve this by uniquely integrating the technique of proxy re-encryption with CP-ABE, and enable the authority to delegate most of laborious tasks to proxy server.

3: Attribute Based data Shearing with attribute revocation

In this paper we focus on an important issue of attribute revocation which is cumbersome for CPABE schemes. In particular, we re-solve this challenging issue by considering more practical scenarios in which semi-trustable on-line proxy servers are available. As compared to existing schemes, our proposed solution enables the authority to revoke user attributes with minimal effort. 4: Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based In existing system we only give the privacy to the data Access control, but not give the user identity privacy, in proposed system we give the privacy to the user identity .In this Scheme we use two scheme Anonym Control, and Anonym Control-F scheme .In this scheme we use the peer-peer protocol.

III. WORKFLOW

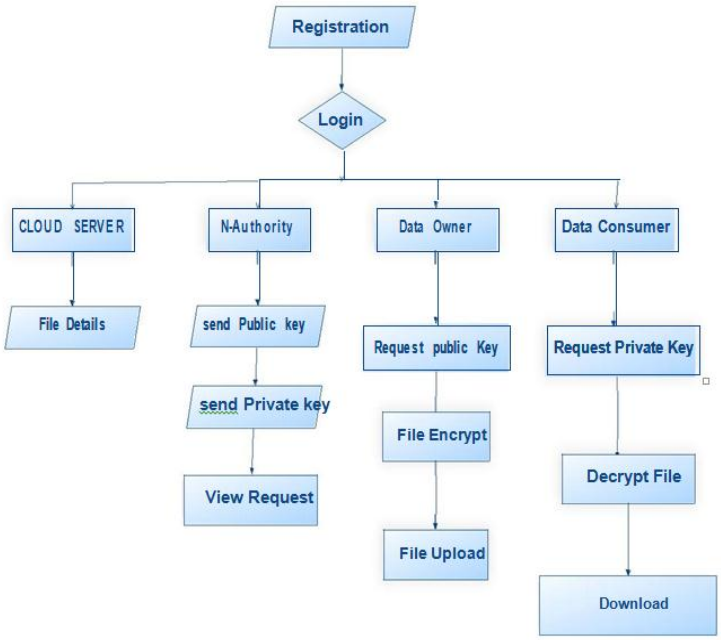

Fig: 2.workflow model

MODULES:

1. Attribute Authorities
2. Data Owners
3. Cloud Server
4. Data Consumers

MODULES DESCRIPTION:

Attribute Authorities:
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. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

Data Consumers:
Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.

Data Owners:
Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies.

Cloud Server:
Then, the owner sends the encrypted data to the cloud server together with the cipher-texts. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user‟s attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

Fully Anonymity Achieved
The key point of the identity information leakage we had in our previous scheme as well as every existing attribute based encryption schemes is that key generator (or attribute authorities in our scheme) issues private key based on the reported attribute, and the generator has to know the user‟s attribute (identities) to do so. We need to introduce a new technique to let key generators issue the correct attribute key without knowing what attributes the users have. The solution is to give all the private keys of all the attributes to the key requester and let him pick whatever he wants. In this way, the key generator does not know which private keys the key requester picked, but we have to fully trust the key requester. To solve this, we leverage the following to Oblivious Transfer (OT). **1-out-of-n oblivious transfer**

In cryptography, an oblivious transfer protocol (**OT**) is a type of protocol in which a sender transfers one of many pieces of information to a receiver, but sender remains oblivious(unware) as what piece of information has been transferred to receiver.In an 1-out-of-n OT, the sender Bob has n messages M1, . . . , Mn , and the receiver Alice wants to pick one Mi from those M1, . . . , Mn . Alice successfully achieves Mi, and Bob does not know which Mi is picked by Alice.

IV. EXPERIMENTAL RESULTS

In this project there are two attribute authorities which can provide private keys against user profile attributes and these authorities can distribute the keys without looking into the user identity information hence anonymity has achieved.

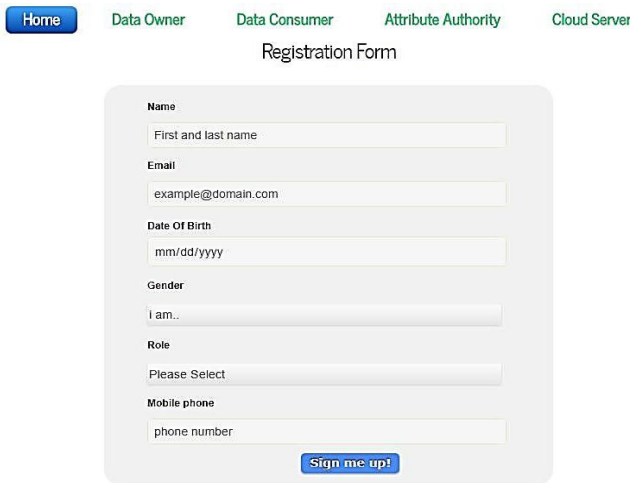

Fig: 3.Registration Page

A user can be a Data Owner and a DataConsumer simultaneously

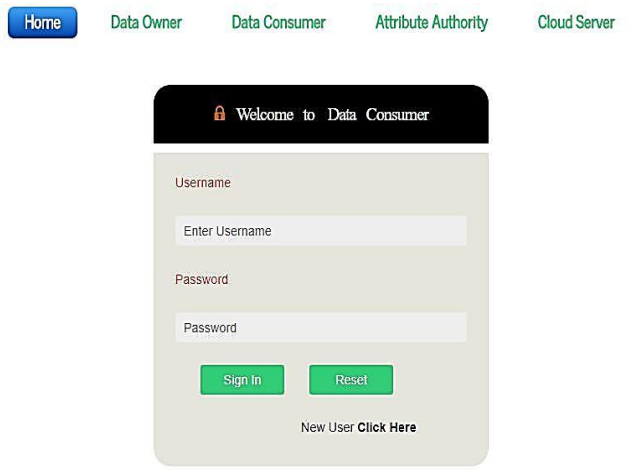

Fig 4: User Login

Attribute authorities generate private keys against attributes of users.

Fig 5: Authority responds

We can create multiple authorities and each authority can select attributes randomly & generate private keys.

V. CONCLUSION

Semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users" identity information. More importantly, our system can tolerate up to N − 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment.

REFERENCES

[1] A. Shamir, "*Identity-based cryptosystems and signature schemes*," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2] A. Sahai and B. Waters, "*Fuzzy identity-based encryption*," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "*Attribute-based encryption for fine-grained access control of encrypted data*," in Proc. 13th CCS, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "*Ciphertext-policy attributebased encryption*," in Proc. IEEE SP, May 2007, pp. 321–334.

[5] M. Chase, *"Multi-authority attribute based encryption*," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[6] M. Chase and S. S. M. Chow, *"Improving privacy and security in multi-authority attribute-based encryption*," in Proc. 16th CCS, 2009, pp. 121–130.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "*Secure threshold multi authority attribute based encryption without a central authority,"* Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

Author's Profile

Thirumanapally Prashanth, is a Ph.D. aspirant and an employee in SC cell Hyderabad. He received his Master of Technology (CSE) in year 2014 from Hasvitha institute of science and technology, RR Dist. Telangana. He received his B.tech (CSE) in year 2012 from Tirumala Engineering college, RR DIst. Telaangana. His field of interest is computer network, Network Security, Cloud Computing and IoT(Internet of Things).

Gundu Purna Chandar Rao is a Research Scholar (Ph.D.) from department of CSE, University college of Engg. Osmania university. He received his master of computer appilications in year 2010 from Horizon Inst. Of Tech. BSc. From EVR Degree and PG college. His field of interest are computer networks, Network Security,Cloud Computing .

