AIJREAS VOLUME 1, ISSUE 7 (2016, JULY) (ISSN-2455-6300) ONLINE
ANVESHANA'S INTERNATIONAL JOURNAL OF RESEARCH IN ENGINEERING AND APPLIED SCIENCES

DATA APPROACH PRIVILEGE BY USING ATTRIBUTE BASED ENCRYPTION IN THE CLOUD

P.BHANU PRAKASH
M. Tech, Department of CSE
Annamacharya Institute of Technology & Sciences,
Tirupathi.
E-Mail: bhanuprakash.pakala13@gmail.com

G.LAKSHMI NARAYANA. Ph. D.,
Assistant professor, Dept. of CSE,
Annamacharya Institute of Technology & Sciences
Tirupathi.
E-Mail: laxminarayana0526@gmail.com

ABSTRACT

Cloud computing is a progressive registering worldview which empowers adaptable, on-interest and minimal effort utilization of figuring assets, yet the information is outsourced to some cloud servers, and different protection concerns rise up out of it. Different schemes in light of the Attribute-Based Encryption have been proposed to secure the distributed storage. Nonetheless, most work focus on the data contents privacy and the access control, while less consideration is paid to the benefit control and the identity privacy. In this paper, we show a semi-anonymous privilege control scheme . Anony Control to address the information protection as well as user identity privacy in existing access control schemes. Anony Control decentralizes the central authority to restrain the identity spillage and in this way accomplishes semi-anonymity. Additionally, it likewise sums up the file access control to the privilege control, by which benefits of all operations on the cloud information can be overseen in a fine-grained way. Subsequently, we exhibit the Anony Control-F which completely keeps the identity spillage and accomplish the full anonymity. Our security analysis demonstrates that both Anony Control and Anony Control-F are secure under the DBDH supposition, and our execution assessment shows the feasibility of our schemes.

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 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.

In the KP-ABE [3], a ciphertext is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user's identity. A user can decrypt the ciphertext if and only if the access tree in his private key is satisfied by the attributes in the ciphertext. However, the encryption policy is described in the keys, so the encrypter does not have entire control over the encryption policy. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when a re-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation. On the other hand, those problems and overhead are all solved in the CP-ABE [4]. In the CP-ABE, ciphertexts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the ciphertext if and only if his attributes in the private key satisfy the access tree specified in the ciphertext. By doing so, the encrypter holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots.

Unlike the data confidentiality, less effort is paid to protect users' identity privacy during those interactive protocols. Users' identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes. But it seems natural that users are willing to keep their identities secret while they still get their private keys.

II. 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).The work by Lewko *et al.* and Muller *et al.* are the most similar ones to ours in that they also tried to decentralize the central authority in the CP-ABE into multiple ones.

Lewko *et al.* use a LSSS matrix as an access structure, but their scheme only converts the AND, OR gates to the LSSS matrix, which limits their encryption policy to boolean formula, while we inherit the flexibility of the access tree having threshold gates. Muller *et al.* also supports only Disjunctive Normal Form (DNF) in their encryption policy.

Disadvantages of Existing System

The identity is authenticated based on his information for the purpose of access control (or privilege control in this paper).Preferably, any authority or server alone should not know any client's personal information.

The users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation.

III. PROPOSED SYSTEM

The data confidentiality, less effort is paid to protect users' identity privacy during those interactive protocols. Users' identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes.

We propose Anony Control and Anony Control-Fallow cloud servers to control users' access privileges without knowing their identity information. In this setting, each authority knows only a part of any user's attributes, which are not enough to figure out the user's identity.

The scheme proposed by Chase et al. Considered the basic threshold-based KP-ABE. Many attribute based encryption schemes having multiple authorities have been proposed afterwards.

In our system, there are four types of entities: *N Attribute Authorities* (denoted as *A*), *Cloud Server*, *Data Owners* and *Data Consumers*. A user can be a Data Owner and a Data Consumer simultaneously.

Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into *N* is joint sets and controlled by each authority, therefore each authority is aware of only part of attributes.

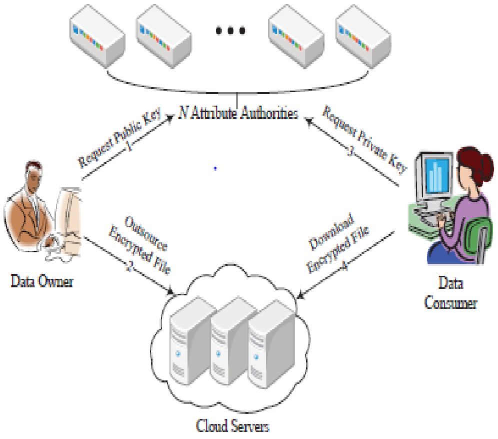
Advantages of Proposed System:

The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in *Anony Control* and no information is disclosed in *Anony Control-F*.

The proposed schemes are tolerant against authority compromise, and compromising of up to *(N* −2*)* authorities does not bring the whole system down.

We provide detailed analysis on security and performance to show feasibility of the scheme *Anony Control* and *Anony Control-F*.

We firstly implement the real toolkit of a multiauthority based encryption scheme *Anony Control* and *AnonyControl-F*.



We propose Anony Control and Anony Control-F (Fig. 1) to allow cloud servers to control users' access privileges without knowing their identity information.

Their main merits are:
1) The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in Anony Control and no information is disclosed in Anony Control-F.
2) The proposed schemes are tolerant against authority compromise, and compromising of up to (N -2) authorities does not bring the whole system down.
3) We provide detailed analysis on security and performance to show feasibility of the scheme AnonyControl and AnonyControl-F.
4) We firstly implement the real toolkit of a multi-authority based encryption scheme AnonyControl and AnonyControl-F.

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

IV. 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.

V. CONCLUSION

This paper proposes a semi-anonymous attribute-based privilege control scheme Anony Control and a fully-anonymous attribute-based privilege control scheme Anony Control-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. We also conducted detailed security and performance analysis which shows that Anony-Control both secure and efficient for cloud storage system. The Anony Control-F directly inherits the security of the Anony Control and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes that support efficient user revocation is one of our future works.

REFERENCES

[1]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.

[2] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," *Int. J. Comput. Math.*, vol. 89, no. 3, pp. 268–283, 2012.

[3] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in *Proc. IEEE 7th SOSE*, Mar. 2013, pp. 573–577.

[4] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2895–2903. JUNG *et al.*: CONTROL CLOUD DATA ACCESS PRIVILEGE AND ANONYMITY 199

[5] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[6] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," *Bull. Korean Math. Soc.*, vol. 46, no. 4, pp. 803–819, 2009.

[7] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multiauthority ciphertext-policy attribute-based encryption with accountability," in *Proc. 6th ASIACCS*, 2011, pp. 386–390.

[8] H. Ma, G. Zeng, Z. Wang, and J. Xu, "Fully secure multi-authority attribute-based traitor tracing," *J. Comput. Inf. Syst.*, vol. 9, no. 7, pp. 2793–2800, 2013.

[9] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public-Key Cryptography*. Berlin, Germany: Springer-Verlag, 2013, pp. 162–179.

[10] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 11, pp. 2171–2180, Nov. 2013.

P. Bhanu Prakash did her bachelor of Technology in Computer Science and Engineering at and doing Master of Technology in Computer Science & Engineering at AITS, Karakambadi, Tirupati, Chittoor, and Andhra Pradesh, India

G. Lakshmi Narayana, did his bachelor of Technology in Information Technology at Narayana Engineering College, had done Master of Technology in Computer Science & Engineering at SV University, and had done Phd., at SV University, Tirupati, Chittoor, and Andhra Pradesh, India.