International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-4,April 2016
ISSN: 2395-3470
www.ijseas.com

A NEWFANGLED ROLE-BASED SYSTEM ON HIERARCHICAL ATTRIBUTE-BASED ENCRYPTION IN CLOUD STORAGE

K. Revathi[1], B. Subashree [2] , R. Sowmya[3]

[1] Assistant Professor/CSE , Dhanalakshmi College of Engineering

[2,3] B.E.-Student, Dhanalakshmi College of Engineering

***Abstract*— The cloud computing draws attention to its security challenges, which are particularly exacerbated due to resource sharing. Due to sharing of physical resources among potential untrusted tenants, cloud computing's multitenancy and virtualization features pose unique security and access control challenges. Additionally, the interference of multitenancy computation can result in unauthorized information flow. Heterogeneity in cloud computing services demands varying degrees of granularity in access control mechanisms. In order to prevent such attacks, a fine-grained authorization mechanism is assisted. From a security management perspective, the goal is to meet cloud users' access control requirements.**

Keywords— Security, Role-based cryptosystem , Fine-grained authorization, Access control.

I. INTRODUCTION

Cloud computing is a progressive computing technique, which provides resources dynamically via Internet. The data storage and computation are outsourced to some party in a 'cloud'. Privacy risks would rise intensely because the servers might illegally inspect users' data and access sensitive information.

Security issues ascended due to the fact that cloud-based storage is outsourcing and they may incur untrusted or honest-but-curious attacks. To provide data access control for cloud storage services. attribute-based encryption (ABE) has been proposed to protect the privacy of consumers' data. However, ABE also has some implementation issues to construct the data access policies. First, data migration from existing IT systems to a cloud storage environment is not easy to be transferred because these systems are usually not designed for ABAC. Second, ABE as a fine-grained data access control requires that "objects receive their attributes either directly from the data creator or as a result of automated scanning tools" according to NIST's ABAC definition. Using role-based model includes simplicity, easy-to-use, and automatic running without user's intervention. Administrator usually specifies role's responsibilities and relationships to other roles using RBAC model. Users need not develop access policies for their own resources; but when necessary, they can customize their own policies.

The conversion from RBAC based rules into ABAC-based policies, can help migrate the data from existing RBAC systems into ABE-based secure cloud storage. In this proposal, an effective cryptographic method to realize partial ordering relation (derived from hierarchy structure in RBAC) has been used by existing ABE solutions. In this approach, a hierarchical hash function (HHF) is introduced for realizing the cryptographic order-preserving mapping from a partial-order hierarchy. Based on this function, a new ABE scheme, called ABE with Attribute Hierarchy (ABE-AH) is presented, for RBAC-compatible data access control for secure cloud storage services. Compared with prior ABE solutions, ABE-AH scheme provides more succinct and richer policy representations with more flexible access control capabilities.

II RELATED WORKS

A. RBAC Model

In an information system, a hierarchy or lattice is used to denote the relationships and arrangements of the objects, users, elements, values, and so on. Especially, in many access control systems the users are organized in a hierarchy constructed with a number of classes, called security classes or roles, according to their competencies and responsibilities. This hierarchy arises from the fact that some users have more access rights than others. In order to manage large-scale systems, the hierarchy in RBAC becomes

more complex than other systems. Especially, role hierarchy (RH) is a natural means for structuring roles to reflect an organization's lines of authority and responsibility.

B. ABAC Model

Similar to role hierarchy in RBAC, the hierarchy is also extremely useful for ABE to introduce attribute hierarchy or attribute lattice (AH or AL), which defines a seniority relation among all values of an attribute, whereby a user holding the senior attribute values acquires the permissions of their juniors. In fact, this kind of attribute lattice has been introduced in ABAC model.

III PROPOSED SYSTEM

In this proposed system, a practical solution is provided to convert RBAC based rules into ABAC-based policies. This conversion can help migrate the data from existing RBAC systems into ABE-based secure cloud storage. An effective cryptographic method is presented to realize partial ordering relation (derived from hierarchy structure in RBAC) used by existing ABE solutions. In our approach, a hierarchical hash function (HHF) is introduced for realizing the cryptographic order-preserving mapping from a partial-order hierarchy. Based on this function, we present a new ABE scheme, called ABE with Attribute Hierarchy (ABE-AH), for our RBAC-compatible data access control for secure cloud storage services. Compared with prior ABE solutions, ABE-AH scheme provides more succinct and richer policy representations with more flexible access control capabilities.

IV ALGORITHM

A. DES (Encryption / Decryption) :

The Data Encryption Standard (DES) is a symmetric key block cipher published by the National Institute of Standards and Technology (NIST).For DES, data are encrypted in 64-bit block using a 56-bit key.DES uses both transposition and substitution and hence referred as a **product cipher.** Data Encryption Algorithm transforms 64-bit input in a series of steps into a 64-bit output.

To decipher it is only necessary to apply the same algorithm to an enciphered message block, taking care that at each iteration of the computation the same block of key bits K is used during decipherment as was used during the encipherment of the block only in a reverse order

B. HMAC Signatures:

HMAC, Hash Based Message Authentication Codes are used between two parties who share a secret key in order to validate information transferred among these parties. We introduce HMAC in storage nodes to demonstrate how to apply the proposed mechanism such that only authorized mobile nodes can securely and efficiently manage the confidential data in the disruption-tolerant military network.

V SYSTEM MODEL

This model focuses on the solution of migrating and sharing the data in existing RBAC systems into cloud. Two problems are resolved in this system: 1) how to remain access constraints of data on RBAC to implement data sharing in cloud; and 2) how to ensure the security of data in public cloud, especially for "honest and curious" cloud .

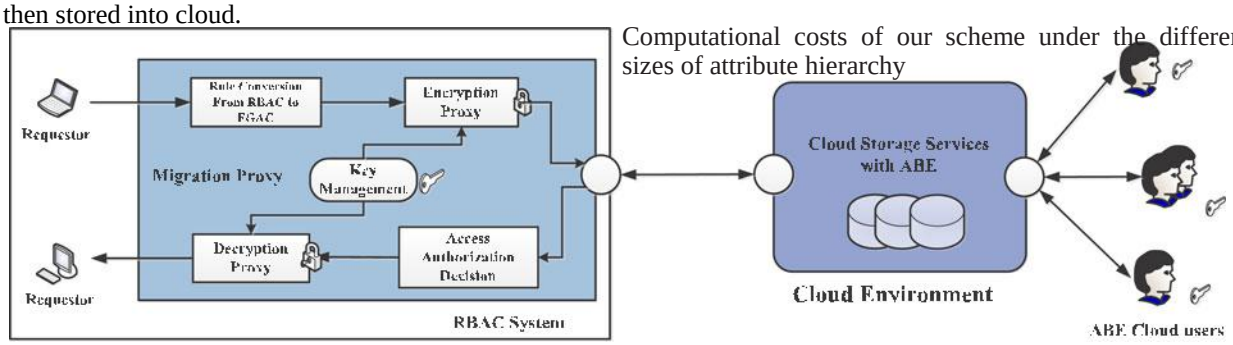
ABAC model is considered as a suitable solution for secure information sharing in large-scale organizations, especially for cloud computing environments. However, facing with a variety of existing enterprise RBAC systems, reestablishment of such a ABAC system is not realistic.

Therefore, a new "transparent" migration solution is developed that existing RBAC systems are integrated into the cloud to implement better data sharing. In this solution, a ABAC-based system is deployed in the cloud, existing RBAC systems are unified into this cloud ABAC system.

The openness of cloud computing means that more authorized users have quick and easy access to the cloud data they need. Furthermore, the ABE cryptosystem must be used for data security in cloud ABAC system. Hence, the goal of this model is to improve ABE for implementing cloud data encryption in the existing RBAC systems.

In order to achieve this goal, we expect to provide an effective method that transforms the RBAC mechanism into an ABE-based instance. Based on

this instance, data can be encrypted by using ABE and then stored into cloud.

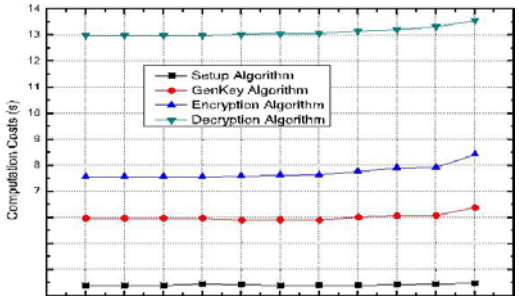


The framework of RBAC-Compatible ABE for secure cloud storage.

In the above fig ,the framework of this solution is discussed, where
a user can use the existing system with RBAC (such as Windows, Linux) to access cloud resources. The accessing process is completely transparent to the user, at the same time, data can be stored and shared by using ABE encryption. In this figure, an existing RBAC system is connected to cloud storage service on ABAC model. To migrate RBAC data to cloud, a new module, called migration proxy, need to append into RBAC system. The proxy can perform the following functions: rule conversion between RBAC and ABAC, encryption/decryption processes, and key management.

VII PERFORMANCE EVALUATION

Our ABE scheme is constructed on bilinear map system from elliptic curve pairings. For simplification, we give several notations to denote the time for various operations in our ABE scheme. E(G) and E(GT) are used to denote the exponentiation in G and GT, respectively. B is used to denote the paring e: GXG->GT. We neglect the operations in Zp, the hash function H: {0,1}* ->G and the multiplication in G and GT, since they are much more efficient than exponentiation and paring operation. We analyse the computation and communication complexity for each phase, where |T | denotes the number of the leaf nodes in the tree, |A| denotes the set of attributes of encryptor and decryptor, and lZp , lG, lGT



Computational costs of our scheme under the different sizes of attribute hierarchy

denote the length of elements in Zp*,G,GT, respectively. The security of comparison operations is based on two mathematical assumptions: the hardness of CDH and eDDH problem, so we define k=80bit
and p=160bit to build a sufficiently secure system

VIII CONCLUSION

In this paper, an effective method is addressed to simplify the policy-specified burden of cloud users in the process of using ABE. Our method is to improve ABE to support RBAC model, the existing RBAC users, without alterations, can access their ABE encrypted data in the cloud. Compared with trivial equal and bit matching in prior solutions, our scheme enhances the expressive capacity of access policies, decreases the computational overheads, and reduces the size of cipher-texts and private-keys for attribute-based encryption.

IX REFERENCES

[1] F. R. Institute. (2010). Personal data in the cloud: A global survey
of consumer attitudes [Online]. Available: http://www.fujitsu.
com/downloads/SOL/fai/reports/fujitsu/personal-data-in-the-cloud.pdf
[2] K. Ren, C. Wang, andQ. Wang, “Security challenges for the public
cloud,”IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb.
2012.
[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted
data,” in Proc. 13th ACM Conf. Comput. Commun. Security,
2006, pp. 89–98.
[4] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-

based encryp-tion with non-monotonic access structures," in Proc. 14th ACM
Conf. Comput. Commun. Security, 2007, pp. 195–203.
[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,
and fine-grained data access control in cloud computing," inProc.
IEEE Conf. Comput. Commun., 2010, pp. 534–542.
[6] R. Bobba, O. Fatemieh, F. Khan, A. Khan, C. A. Gunter, H. Khur-ana, and M. Prabhakaran, "Attribute-based messaging: Access
control and confidentiality,"ACM Trans. Inf. Syst. Secur., vol. 13,
no. 4, p. 31, 2010.
[7] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller,
and K. Scarfone, "Guide to attribute based access control (ABAC)
definition and considerations, "NIST Special Publ., vol. 800, p. 162,
2014.
[8] M. J. Atallah, K. B. Frikken, and M. Blanton, "Dynamic and effi-cient key management for access hierarchies," inProc. 12th ACM
Conf. Comput. Commun. Security, Alexandria, VA, USA, 2005,
pp. 190–202.
[9] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and
P. Samarati, "Over-encryption: Management of access control evo-lution on outsourced data," inProc. 33rd Int. Conf. Very Large Data
Bases, 2007, pp. 123–134.
[10] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A
practically motivated enhancement to attribute-based
encryption," inProc. 15th Eur. Symp. Res. Comput. Security, 2009,
pp. 587–604.
[11] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryp-tion for fine-grained access control in cloud storage services,"
inProc. ACM Conf. Comput. Commun. Secur., 2010, pp. 735–737.
[12] J. Li, Q. Wang, C. Wang, and K. Ren, "Enhancing attribute-based
encryption with attribute hierarchy," inProc. ACM Mobile Netw.
Appl., vol. 16, no. 5, pp. 553–561, 2011.
[13] Y. Zhu, G.-J. Ahn, H. Hu, D. Ma, and S. Wang, "Role-based cryp-tosystem: A new cryptographic RBAC system based on role-key
hierarchy," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 12,
pp. 2138–2153, Dec. 2013.
[14] R. Sandhu, E. Coyne, H. Fenstein, and C. Youman, "Role-based
access control models,"IEEE Comput., vol. 29, no. 2, pp. 38–47,
Feb. 1996.
[15] R. Bobba, O. Fatemieh, F. Khan, C. A. Gunter, and H. Khurana,
"Using attribute-based access control to enable attribute-based
messaging," inProc. 22nd Annu. Comput. Security Appl. Conf., 2006,
pp. 403–413.
[16] A. Sahai and B. Waters, "Fuzzy identity-based encryption,"
inProc. EUROCRYPT, 2005, pp. 457–473.
[17] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attri-bute-based encryption," inProc. IEEE Symp. Secur. Privacy, 2007,
pp. 321–334.
[18] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext
policy attribute based encryption," inProc. Int. Colloq. Automata,
Lang. Program., 2008, pp. 579–591.
[19] Y. Zhu, G.-J. Ahn, H. Hu, S. Yau, H. An, and C.-J. Hu, "Dynamic
audit services for outsourced storages in clouds," IEEE Trans.
Serv. Comput., vol. 6, no. 2, pp. 227–238, Apr.-Jun. 2013.
[20] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving
encryption for numeric data," inProc. ACM SIGMOD Int. Conf.
Manage. Data, 2004, pp. 563–574.
[21] A. Boldyreva, N. Chenette, and A. O'Neill, "Order-preserving
encryption revisited: Improved security analysis and alternative
solutions," in Proc. Annu. Int. Cryptol. Conf. Adv. Cryptol., 2011,
pp. 578–595.
[22] D. Boneh and M. Franklin, "Identity-based encryption from the
weil pairing," inProc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol.,
2001, pp. 213–229.