ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Secure Sharing Of Related Organization Records in Cloud Computing

S.Keerthana[1]

ME, Department of ECE, EBET Group Of Institutions, Kangayam, Tirupur Dt, Tamilnadu, India[1]

Abstract: Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing. The proposed scheme is not only achieves scalability due to its hierarchical structure, also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. This method is used to access the single dataset or local dataset from the cloud computer. In proposed system, data interoperation systems integrate information from different local sources to enable communication and exchange of data between them. A common model for these systems involves a global representation of the local data, which acts as a mediator for translating queries and conveying data to and from these sources using the global-as view approach. In addition, global resource employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. It formally proves the security of global resource based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme and analyzes its performance and computational complexity.

Keywords: cloud providers, attribute-based encryption (ABE), ciphertext-policy attribute-based encryption (CP-ABE), public key encryption (PKE), and Resource description frame work (RDF).

I. INTRODUCTION

The notion of ABE is a new method for fuzzy identity-based encryption. The primary drawback of the scheme is that, its threshold semantics lacks expressibility. Several efforts followed in the literature is try to solve the expressibility problem. In the ABE scheme, ciphertexts are not encrypted to one particular user as in traditional public key cryptography. Rather, both ciphertexts and users decryption keys are associated with a set of attributes or a policy over attributes. A user is able to decrypt a ciphertext only if there is a match between his decryption key and the ciphertext. ABE schemes are classified into key-policy attribute-based encryption (KP-ABE) and (CP-ABE), depending how attributes and policy are associated with ciphertexts and users decryption keys.

In a KP-ABE scheme, a ciphertext is associated with a set of attributes and a users decryption key is associated with a monotonic tree access structure. Only if the attributes associated with the ciphertext satisfy the tree access structure, the user can decrypt the ciphertext. In a CP-ABE scheme, the roles of ciphertexts and decryption keys are switched. The ciphertext is encrypted with a tree access policy chosen by an encryptor, while the corresponding decryption key is created with respect to a set of attributes. As long as the set of attributes associated with a decryption, key satisfies the tree access policy associated with a given ciphertext and the key can be used to decrypt the ciphertext. Since users decryption keys are associated with a set of attributes, CP-ABE is conceptually closer to traditional access control models such as Role-Based Access Control (RBAC). Thus, it is more natural to apply CP-ABE, instead of KP-ABE, to enforce access control of encrypted data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

II. EXISTING SYSTEM

Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, utility computing, and service oriented architecture. Although the great benefits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and potential cloud users, security problems in cloud computing become serious obstacles which, without being appropriately addressed, will prevent cloud computings extensive applications and usage in the future. To achieve flexible and fine-grained access control, a number of schemes have been proposed [9] and [11]. Unfortunately , these schemes are only applicable to systems in which data owners and the service providers are within the same trusted domain. Since data owners and service providers are usually not in the same trusted domain in cloud computing, a new access control scheme employing attributed-based encryption. The notion of ABE was first introduced in [11] as a new method for fuzzy identity-based encryption. The primary drawback is that its threshold semantics lacks expressibility. Several efforts followed in[8],[9] and [11] inorder to solve the expressibility problem.

In the ABE scheme, ciphertexts are not encrypted to one particular user as in traditional public key cryptography. Rather, both ciphertexts and users' decryption keys are associated with a set of attributes or a policy over attributes. A user is able to decrypt a ciphertext only if there is a match between users decryption key and the ciphertext. ABE schemes are classified into (KP-ABE) and (CP-ABE), depending how attributes and policy are associated with ciphertexts and users decryption key.

III. PROPOSED SYSTEM

The main objective is to improve the scalability and security. For that purpose ABE is used. The process of mapping security levels associated with the elements of the local schemas to (RDF) schema triples. The local security policies are represented as local security lattices associated with both the local and the RDF schema levels. Local security lattices are merged into a global security lattice representing the global security levels associated with the global RDF schema. Access control models have been the focus of recent research, including approaches in which the access control model is expressed in terms of tuples. For security purpose and access control global resource attribute-set-based encryption scheme is used in cloud computing. Global resource attribute-set-based encryption extends the ciphertext-policy attribute- set-based encryption scheme with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control. It consists of five types of parties as cloud service provider, data owners, data consumers, a number of domain authorities, and a trusted authority. The cloud service provider manages a cloud to provide data storage service.

3.1 RDF

The Resource Description Framework (RDF) is a family of World Wide Web Consortium(W3C) specifications originally designed as a metadata data model. It has come to be used as a general method for conceptual description or modeling of information that is implemented in web resources, using a variety of syntax notations and data serialization formats.

3.2 AES

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. It is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST has selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths as128, 192 and 256 bits. The

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

algorithm described by AES is a symmetric-key algorithm. The same key is used for both encrypting and decrypting the data.

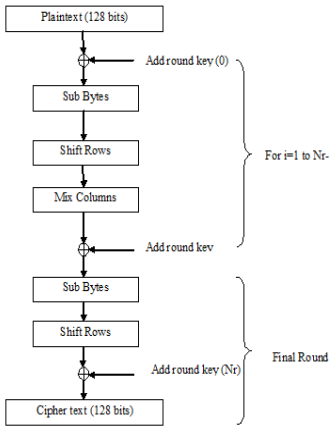

Figure: 3.2 AES Encryption part

3.2.1 Sub Bytes

In the sub bytes step, each byte ($a_{i,j}$) in the state matrix is replaced with a Sub Byte $S(a_{i,j})$ using an 8-bit substitution box, the Rijndael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over GF (2^8), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen to avoid any fixed points.

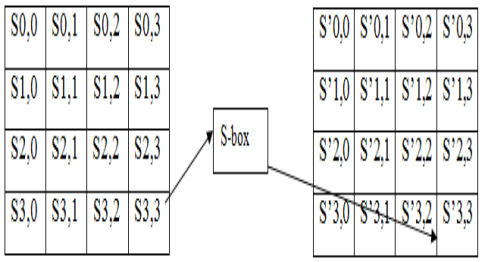

Figure: 4.2.1 Sub Bytes

3.2.2 Shift Rows

In the shift rows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row. The shift rows step operates on the rows of the state which cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged and each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row 'n' is shifted left circular by 'n-1' bytes. In this way, each column of the output state of the Shift Rows step is composed of bytes from each column of the input state.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

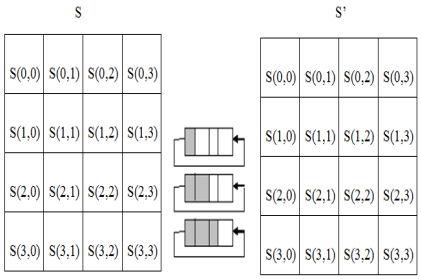

Figure:3.2.2 Shift Rows

For a 256-bit block, the first row is unchanged and the shifting for the second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively. This change only applies for the Rijndael cipher when used with a 256-bit block, as AES does not use 256-bit blocks. The importance of this step is to avoid the columns being linearly independent, in which case, AES degenerates into four independent block ciphers.

3.2.3 Mix Columns

In the mix columns step, the four bytes of each column of the state are combined using an invertible linear transformation . The mix columns function takes four bytes as input and four bytes as output where each byte affects all four output bytes.

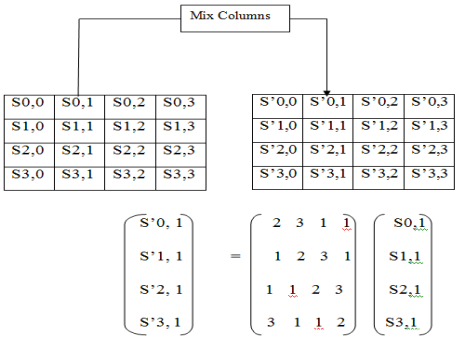

Figure:4.2.3 Mix Columns

3.2.4 Add Round Key

In the addroundkey step, the sub key is combined with the state. For each round, a sub key is derived from the main key using Rijndaels schedule. Each sub key is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the sub key using bitwise XOR.

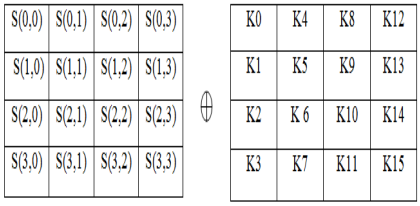

Figure: 3.2.4 Add Round Key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. RESULT

For using 128 bit in AES algorithm has 10 rounds. Each round using the four transformations and the final round does not use the mix column operation. The following figure shows the final output

REFERENCES

[1]. M. Li, S. Yu, K. Ren, and W. Lou, (2010) "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106,.

[2]. H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, (2010)"Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229.

[3]. M. Li, S. Yu, N. Cao, and W. Lou, (2011)"Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11).

[4]. "The Health Insurance Portability and Accountability Act," http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp 2012.

[5]. "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6]. "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing about How Well Privacy Can Be Safeguarded," http://articles.latimes.com/2006/jun/26/health/he-privacy26, 2006.

[7]. K.D. Mandl, P. Szolovits, and I.S. Kohane, (2011)"Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287,.

[8]. J.Benaloh, M. Chase, E. Horvitz, and K.Lauter,[2012] "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114.

[9]. S. Yu, C. Wang, K. Ren, and W. Lou,(2010) "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10.

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

[11]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, (2006)"Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98,

[12]. M. Li, W. Lou, and K. Ren, (2010)"Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58,.