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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Anonymous Authentication of Data Stored In Clouds for Decentralized Access Control

Remya s s

M.Tech Student, Dept of CSE, Lourdes Matha College of Science and Technology, Trivandrum, India

ABSTRACT: This paper propose a decentralized access control scheme that provide a secure data storage in clouds. In this scheme before storing data in cloud check or clarify the authenticity of the user without knowing its identity. The stored data's are decrypted only possible by registered users. This scheme also prevent replay attacks and allow creation, modification, and reading stored data to and from the cloud. This paper also address the user revocation. The other control schemes are centralized but this paper introduce authentication and access control scheme is decentralized and robust. The scheme result is more secure data storage in clouds and support anonymous authentication.

KEYWORDS: Access control; Authentication; Attribute-based signatures; Attribute-based encryption; Cloud storage.

I. INTRODUCTION

Review in Cloud computing has accepted a lot of rewards from classical and economic worlds. In cloud computing users can arrangement their estimation and in reserve to clouds using Internet. The services like appositeness, framework and arenas are provided by cloud and helps organizers to write application. The data encryption process is used for the secure data storage. The data stored in cloud is commonly altered so this characteristics is to be deliberate while conniving the accomplished protected reserve techniques. In clouds, important concern is that properly searching on encrypted data. The cloud reviewers have made up protectively and concealment preservation in cloud. Personal information, images and videos are allowed to access and store only by valid user and all this data's are stored in cloud. The goal of this paper is not just store the data securely in cloud it is also important to make secure that anonymity of user is ensured. The situation like user wants to comment on object but does not want to be known. But the customer wants the other customer that he is a genuine user. In this paper scheme used two protocols that are Attribute Based Encryption (ABE) and Attribute Based Signature (ABS). ABE and ABS are combined to offer authoritative access control without communicating the community of the user.

The main features of this paper are the following: 1) Delivered access control of input gatheredin cloud so that only approved users with valid features can access them. 2) Confirmation of users who gather and change their data on the cloud. 3) The integrity of the user is secured from the cloud during certification. 4) The constructionis decentralized, explanationthat there can be various KDCs for key administration. 5) The access control and certification are both conspiracy defiant, explanation that no two users can collaborate and access data or certificate themselves, if they are independently not authorized. 6) Cancelled users cannot access data after they have been cancelled. 7) The proposedscheme is volatile to replay intrusion. A writer whose features and keys have been cancelled cannot write back decayed data. 8) The protocol supports numerous read and write on the information reserved in the cloud. 9) The expenses are proportionate to the existing centralized approaches, and the expenditure operations are mostly done by the cloud.

II. RELATED WORK

In ABE [1], a customer has a group of features in addition to its unique ID. This paper introduce two classes of ABE ´ s that are Key-policy ABE or KP-ABE [2] and Cipher text-policy or CP-ABE [3]. KP-ABE shows the user has an access policy to encrypt information. A writer whose features and keys have been cancelled cannot write back decayed information. The accepter accepts features and secret keys from the feature authority and is able to decrypt

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

data if it has matching features. CP-ABE shows that the acceptor has the access policy in the form of tree with features as the leaves.
The existing approaches take centralized approach and only take one KDC. This will be chases the [4] [11] multi-authority ABE that shows that it take multiple KDC authorities which broadcast features and secret keys to customers. Recently, proposed fully decentralized ABE [5] where customers could have zero or more features from each authority and do not require a faithful sender. Attribute Based Signature scheme [6][12] takes a decentralized approach and provides authentication without disclosing the integrity of the customers.

III. PROPOSED METHOD

Information stored in cloud follows Distributed access control scheme so that only authorized customers with valid features can access the information. Authentication of customers performs stock and accommodation of the information in the cloud. During certification the integrity of the customer is protected from the cloud. The cloud architecture is decentralized, which means that there can be several KDCs for key management. The both access control and certification schemes are collaborate resistant. The collaborate resistant attack means that no two users can collaborate and access information or authenticate themselves, even though they are individually not authorized. Cancelled [8] users cannot access information after he/she have been cancelled.
The benefits of the proposed systems are delivered access control of information stored in cloud so that only certified customers with valid features can access them. Certification of customers who store and modify their information on the cloud. The integrity of the customer is protected from the cloud during certification [10].
This paper proposes privacy preserving certificated access control scheme. According to this scheme a customer can create a file and store it securely in the cloud. This scheme uses two protocols that are ABE and ABS.

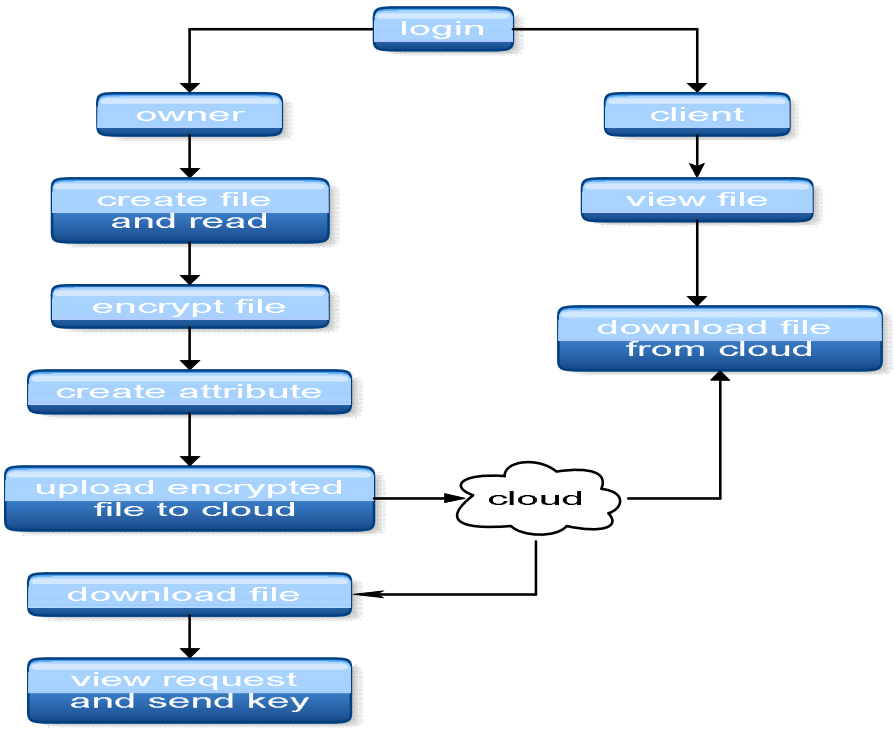

Figure: 1-Architecture of proposed system

The above fig shows that first the owner create a file and then encrypt the file and create the attribute to each file. This file then upload to cloud. The client view the file and download the file from cloud. Any changes will appear or

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

modify then the owner first decrypt the encrypted data and then modified it. The proposed system includes following techniques:

A. *Cloud uploading:*
In this module important files and documents are uploaded to cloud space using Smart File cloud service provider. This cloud service provider, provide free cloud space where we can place our records. In this procedure we use a cloud file API(smart file) and a library file in support. It provides a vast space for data storage. File transferring and sharing can also possible by uploading file to cloud.

B. *File Encryption:*
In cloud computing the main disadvantage is, it doesn't contain any security. So for avoiding this we use a file encryption strategy, which helps the file owner to keep their file secure. For high security encryption, the system uses AES Algorithm, which is top most algorithms in the case of file security suggested by NASA. In our work, attributes are the key for AES encryption.

C. *File Decryption:*
In file decryption AES decryption standard is used. While downloading file from cloud the client should need, the access permission from the owner, based on their attributes. Access permission is assigned by sending them a permission key to their mail id. When they try to download the cloud file system ask them to enter the key. If the key matches then the system will check whether the account holder is a proper one and the assigned one to achieve that file.

D. *Anonymous ID Generation:*
This module helps the user to use the cloud system without revealing their identity. The module generates dynamic tokens as anonymous id for each secured owners with the help of MD5CryptoServiceProvider algorithm which is used for hash code creation. Anonymous id helps the user to share and access data without losing their identity.

IV. PROPOSED ALGORITHM

A. *AES Algorithm:*
The Advanced Encryption Standard (AES), also known as Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemon and Vincent Rijmen, who 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 selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits [9].

AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

B.*AES Algorithm Steps:*

The encryption process uses a set of specially derived keys called round keys. The data to be encrypted. This array we call the state array.

AES steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.

Copy the final state array out as the encrypted data (ciphertext).

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

C.*AES Algorithm Description:*

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4×4 column-major order matrix of bytes [7], termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

For instance, if you have 16 bytes, b0, b1... b15, these bytes are represented as this matrix:

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

D. *High-level description of the algorithm:*

1. Key Expansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

a) Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

b) Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

c) Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

d) AddRoundKey

4. Final Round (no Mix Columns)

a. Sub Bytes

b. Shift Rows

c. AddRoundKey.

V. SIMULATION RESULTS

The result of this paper is high accuracy and more performance level.The scenario was modeled as an optimization problem that aims to maximize the performance by minimizing the execution time depending upon the need of user and was solved using meta-heuristic optimization algorithm, GA. The result obtained is an optimized resource provisioning and scheduling mechanism for Clouds.The result graph 2 of Load and Timing parameters shows the expected variations. GA gives better performance figures for smaller counts of resources, which typically are. Small companies are going for small number of virtual machine requirements and will need less than 10 VM at a time.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

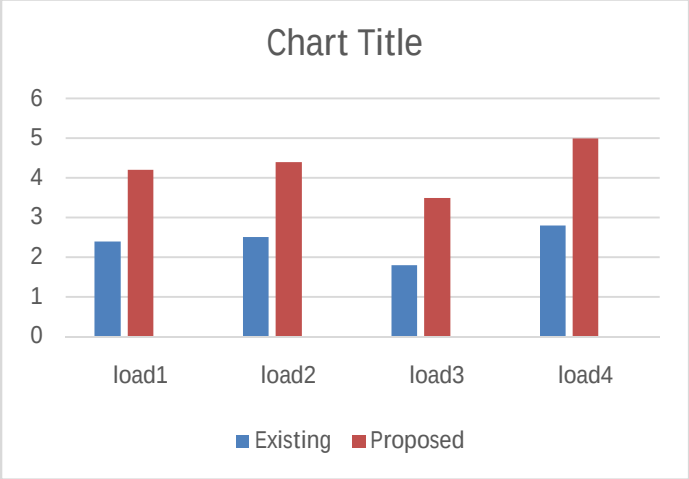

Figure: 2-Result of the load

VI. CONCLUSION AND FUTURE WORK

A combined resource provisioning and scheduling strategy was analyzed for executing scientific work flows on IaaS clouds. The scenario was modeled as an optimization problem that aims to maximize the performance by minimizing the execution time depending upon the need of user and was solved using meta-heuristic optimization algorithm, GA. The result obtained is an optimized resource provisioning and scheduling mechanism for Clouds.One problem is that the cloud knows the access policy for every records reserved in the cloud. In future the attributes and access policy of the user are hide to the cloud.

REFERENCES

1. A.SahaiandB.Waters, "Fuzzy identity-based encryption," inEUROCRYPT, ser. Lecture Notes in Computer Science, vol. 3494. Springer, pp. 457–473, 2005.
2. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, pp. 89–98, 2006.
3. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy. , pp. 321–334, 2007.
4. M. Chase, "Multi-authority attribute based encryption," in TCC, ser. Lecture Notes in Computer Science, vol. 4392. Springer, pp. 515–534, 2007.
5. A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in EUROCRYPT, ser.Lecture Notes inComputer Science, vol.6632. Springer, pp. 568–588, 2011.
6. H. K. Maji, M. Prabhakaran, and M. Rosulek,"Attribute-based signatures," in CT-RSA, ser. Lecture Notes in Computer Science, vol. 6558. Springer, pp. 376–392, 2011.
7. A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," Ph D Thesis. Technion, Haifa, 1996.
8. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ACM ASIACCS, pp. 261–270, 2010.
9. A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in EUROCRYPT, ser.Lecture Notes inComputer Science, vol.6632. Springer, pp. 568–588, 2011.
10. J. Hur and D. Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, 2011.
11. H. Lin, Z. Cao, X. Liang and J. Shao, "Secure Threshold Multi-authority Attribute Based Encryption without a Central Authority," in INDOCRYPT, ser. Lecture Notes in Computer Science, vol. 5365, Springer, pp. 426–436, 2008.
12. H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," IACR Cryptology ePrint Archive, 2008.