ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Efficient Key Management for Enforcing Secure Role Based Access Control on Encrypted Data in Cloud Storage

Sivaprasad Manivannan[1], Muthuselvi[2]

P.G. Student, Department of Computer Science & Engineering, UCEN, Tamil Nadu, India [1]

Assistant Professor, Department of Computer Science & Engineering, UCEN, Tamil Nadu, India [2]

ABSTRACT: In the existing system, role manager give authorization to user when he begins encryption. After that user have all the permission to access the function. The project developed by access provides security by enabling the function of role manager. The role manager monitors every function to provide additional security. It includes two encryption and decryption (One by user and one by role manager. User use public & private key to encrypt and decrypt video, whereas role manager use AES to encrypt and decrypt video. Private Key frameworks utilize the same key to encode and decode information. Open key encryption functions admirably in circumstances where you can't safely impart a key, as over the Internet, however it has some real disadvantages. The main disadvantages of thistechnique are speed, certification problems, direct compromise, and false sense of security. AES encryption is a block cipher that uses an encryption key and a several rounds of encryption. A block cipher is an encryption that works on a single block of data at a time. In the case of standard AES encryption the block is 128 bits, or 16 bytes, in length. The term rounds refer to the way in which the encryption mixes the data re-encrypting it ten to fourteen times depending on the length of the key. The AES encryption itself is not a computer program or computer source code.

KEYWORDS: AES, Encryption systems, Cloud Computing

I. INTRODUCTION

Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry. By combining a set of existing and new techniques from research areas such as Service Oriented Architectures (SOA) and virtualization, cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet.

As promising as it is, cloud computing is also facing many challenges that, if not well resolved, may impede its fast growth. Data security, as it exists in many other applications, is among these challenges that would raise great concerns from users when they store sensitive information on cloud servers. These concerns originate from the fact that cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of the users. Data confidential against cloud servers is hence frequently desired when users outsource data for storage in the cloud. In some practical application systems, data confidentiality is not only a security/privacy issue, but also of juristic concerns. For example, in healthcare application scenarios use and disclosureof protected health information (PHI) should meet the require- Health Insurance Portability and Accountability Act (HIPAA) [5], and keeping user data confidential against the storage servers is not just an option, but a requirement. Furthermore, we observe that there are also cases in which cloud users themselves are content providers. They publish data on cloud servers for sharing and need fine-grained data access control in terms of which user (data consumer) has the access privilege to which types of data. In the healthcare case, for example, a medical center would be the data owner who stores millions of healthcare records in the cloud. It would allow data consumers such as doctors, patients, researchers and etc, to access various types of healthcare records under policies admitted by HIPAA. To enforce these access policies, the data owners on one hand would like to take advantage of the abundant resources that the cloud provides

DOI: 10.15680/IJIRSET.2015.0405095

for efficiency and economy; on the other hand, they may want to keep the data contents confidential against cloud servers. A system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption was presented. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data deter- mines a policy for who can decrypt..

II. RELATED WORK

A. Oblivious Transfer with Hidden Access Control from Attribute-Based Encryption

HACOT scheme which is more efficient and offers more expressive policies was presented in this paper. We construct our HACOT protocol based on a hidden ciphertext-policy attribute-based encryption (HP-ABE) scheme. The goal is to amortize communication costs so that the encrypted database of size linear in is transmitted once. We prove our construction secure by a reduction to the security, the Symmetric External Diffie-Hellman (SXDH) and Simultaneous Flexible Pairing (SFP) assumptions. Private Key frameworks utilize the same key to encode and decode information. Open key encryption functions admirably in circumstances where you can't safely impart a key, as over the Internet, however it has some real disadvantages. The main disadvantages of this technique are speed, certification problems, direct compromise, and false sense of security.

B.**Ciphertext- Policy Attribute- Based Encryption**

A system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption was presented. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data deter- mines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). An alternative formulation of role-based access control that enables us to apply existing cryptographic schemes to core and hierarchical role-based access control policies was presented. Then this paper showed the special cases of our cryptographic enforcement schemes for role-based access control are equivalent to cryptographic enforcement schemes for temporal access control and to ciphertext-policy and key-policy attribute-based encryption schemes. Finally, it describes how these special cases can be extended to support richer forms of temporal access control and attribute-based encryption. The goal is to amortize communication costs so that the encrypted database of size linear in is transmitted once. We prove our construction secure by a reduction to the security, the Symmetric External Diffie-Hellman (SXDH) and Simultaneous Flexible Pairing (SFP) assumptions.

C. **A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments**

I survey a basic attribute-based encryption scheme, two various access policy attribute- based encryption schemes, and two various access structures, which are analyzed for cloud environments. Attributes have been exploited to generate a public key for encrypting data and have been used as an access policy to control users' access. The access policy can be categorized as either key-policy or cipher text-policy. The key-policy is the access structure on the user's private key, and the cipher text-policy is the access structure on the cipher text. And the access structure can also be categorized as either monotonic or non-monotonic one. In Ciphertext-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the ciphertext is associated with an access policy over attributes. The user can decrypt the ciphertext if and only if the attribute set of his secret key satisfies the access policy specified in the ciphertext. Several CP-ABE schemes have been proposed, however, some practical problems, such as attribute revocation, still needs to be addressed.

III. ARCHITECTURE AND ROLEBASED ACCESS CONTROL

It provides a better security solution for accessing data on cloud. Roles in RBAC are mapped to access permissions, and all users are mapped to appropriate roles and receive access permissions only through the roles to which they are assigned, or through hierarchical roles, roles get access permission. Within an organization, there may be number of users and types of permission, whose role and accordingly access differs. Controlling all access through roles gives benefit to organization and it also simplifies the management. Typically, role-based access control model has three essential structures; users permissions and roles. A role is a higher level representation of access control. User correspond to real world users of the computing system. User authorization can be accomplished separately; assigning users to existing roles and assigning access privileges for objects to roles. Permissions gives a description of the access users can have to objects in the system and roles gives a description of the functions of users within an organization. In RBAC, there is hierarchical structure; a role can inherit access permission from another role. The role based access policies are strengthened by using role-based encryption scheme (RBE).In RBE scheme the owner of the data encrypts the data in such a way that only those users can decrypt the data who possess appropriate access permission according to their role specified by role-based access control policies. Role grants permission to access data according to their role and can also revoke the permission from existing user of role. Revoked user will not have any type of access permission to any encrypted data for the role. Revocation of the user does not affect other users and roles in the system. In RBE, four types of entities are used; SA is a system administrator which generates keys to users and roles and provides authorization. RM is a role manager who gives access to user according to their role. Users used to decrypt and access data from cloud. Data are stored on cloud by owner of the data.

1.Role Based Encryption

RBE scheme the owner of the data encrypts the data in such a way that only those users can decrypt the data who possess appropriate access permission according to their role specified by role-based access control policies. Role grants permission to access data according to their role and can also revoke the permission from existing user of role. Revoked user will not have any type of access permission to any encrypted data for the role. Revocation of the user does not affect other users and roles in the system. In RBE, four types of entities are used; SA is a system administrator which generates keys to users and roles and provides authorization. RM is a role manager who gives access to user according to their role. Users used to decrypt and access data from cloud. Data are stored on cloud by owner of the data. In RBE system, following algorithms are used;

Setup(λ): This algorithm takes λ as input and generates master secrete key (mk) and public key (pk).

Extract(mk, ID): SA execute this algorithm. If user identity ID matched, then SA provides mk to the user i.e. if ID = IDu, then SA generates dku which is secrete key of user. If ID is matched with role, SA provides mk to RM. ID = IDR, then SA generates skr which is secrete key of role.

Manage Role(mk, IDR, PRR): SA execute this algorithm to manage role with identity IDR from other role. Here, role hierarchy is maintained. All the roles are stored as a set of PRR. SA generates role public parameter as AR, BR and stored them on cloud.

AddUser(pk, skR, RULR, IDu): RM execute this algorithm in which RM gives role to user and also provides authentication. Role user list RULR is updated in cloud.

RevokeUser(pk, sk, RULR, IDu): RM execute this algorithm and sends user ID IDu to the cloud, then cloud computes some parameters and send them back to RM from which RM replaces old role parameters with new parameters.

Encrypt(pk, pubR): Encryption is done by owner of the data and it stores cipher text C of message m to the cloud. This algorithm takes pk and pubR as input parameters and generates (C, K) tuple where K is used to encrypt original message.

Decrypt(pk, pubR, dku, C): This algorithm is executed by those user who possess access according to their role. This algorithm takes pk, pubR, dku, C as input parameters and generates output by decrypting original message by using K.

Security information can be attached to a network object as a list, recording a group of trusted network objects that are authorized to access other network objects. This is an Access Control List (ACL). Permission is a set of attributes describing the kind of privileges that determine what a network object can do. The administrator assigns permissions to a network object. A permission set contains only the following privileges: Supervisor (S) grants all sorts of rights to an individual network object or group of objects.

Create (C) allows the creation or renaming of a network object.

Delete (D) enables the deletion of a network object.

Read (R) allows a network object to read the content of an object value Write (W) lets a network object write or modify the content of an object state.

Execute (X) enables a network object to execute services (or operations) of other network objects.

2.AES Encryption

AES encryption is a block cipher that uses an encryption key and a several rounds of encryption. A block cipher is an encryption that works on a single block of data at a time. In the case of standard AES encryption the block is 128 bits, or 16 bytes, in length. The term rounds refer to the way in which the encryption mixes the data re-encrypting it ten to fourteen times depending on the length of the key. The AES encryption itself is not a computer program or computer source code. It is a mathematical description of a process of obscuring data. AES encryption is more secure, quicker in both equipment and programming. Also the principle preference of the AES encryption is needed by the most recent U.S. and international standards.

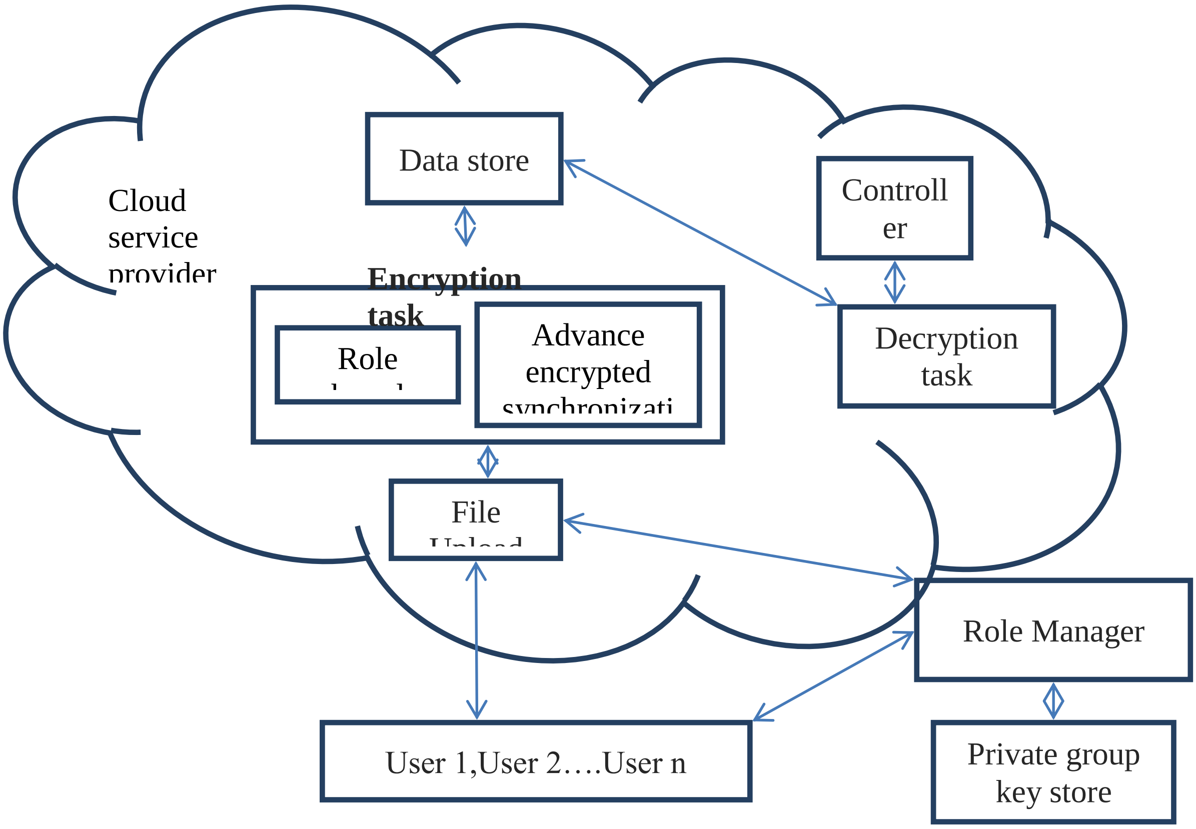

Fig 1. Architecture Diagram for Role Based AES Encryption

3. Advanced Encryption synchronization

AES (Advanced Encryption Standard) The Advanced Encryption Standard specifies a federally-approved algorithm used to protect electronic data, considered strong enough to satisfy Federal Information Processing standards (FIPS). The algorithm encrypts and decrypts information, and is capable of using cryptographic keys of 128, 192 and 256 bits.

Asymmetric Key (Public-Key) is used to encrypt messages (public key), while a private key is used to decrypt them. The private key must be kept secret, while the public key has no risk even if it becomes known to others (the public key is meant to be shared). Storage encryption technology uses cryptographic keys to encrypt and decrypt data. Cryptography is based on computationally secure algorithms designed to protect data.

Cryptographic Hash algorithm that can change a large block of data into a fixed-length string; the cryptographic hash. No two blocks of different data have the same hash. This is an example of one-way encryption. A hacker who obtains the password cannot run the hash through an algorithm to decrypt the password. In Ciphertext the plaintext has been passed through a cryptographic encryption algorithm, ciphertext is the result. Ciphertext is irreversible without the encryption key. Data Encryption Key (DEK) is used for the encryption of plaintext and for the computation of message integrity checks (signatures). Encryption Rendering plaintext into ciphertext, meaning to render original data unreadable or undecipherable. In File Encryption the Individual files are encrypted on a storage medium and are accessible only after proper authentication.

A new role-based encryption (RBE) scheme with efficient user revocation that combines RBAC policies with encryption to secure large scale data storage in a public cloud. A secure RBAC based hybrid cloud storage architecture which allows an organization to store data securely in a public cloud. A non-constant size decryption key will usually make it difficult for the users to decide the memory requirements that are needed on the client devices to store the keys.

Maintaining the sensitive information related to the organization structure in a private cloud. A new access control model is the role-based access control (RBAC), which provides flexible controls and management by having two mappings, users to roles and roles to privileges on data objects be in painted.

IV. CONCLUSIONS & FUTURE WORK

Proposed a RBE and AES schemes are achieves efficient user revocation.Then we presented a RBAC based cloud storage architecture which allows an organisation to stored at a securely in a public cloud, while maintaining the sensitive information related to the organisation's structure in a private cloud. Then we have developed a secure cloud storage system architecture and have shown that the system has several superior characteristics such as constant size ciphertext and decryption key.

- The project developed by access provides security by enabling the function of role manager.
- The role manager monitors every function to provide additional security.
- User use public & private key to encrypt and decrypt video, whereas role manager use AES to encrypt and decrypt video.
- To improve the overall limitations RBAC based AES encryption algorithm is introduced in this paper.
- RM is a role manager who gives access to user according to their role. Users used to decrypt and access data from cloud. Data are stored on cloud by owner of the data.

ACKNOWLEDGMENT

We are grateful to inventors of Role Based who fueled our research into this area. Our special thanks to our respective institutions and guides for encouraging us to pursue research into this area.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

REFERENCES

[1] Jan Camenisch, Maria Dubovitskaya, Robert R. Enderlein and Gregory Neven, “Oblivious Transfer with Hidden Access Control from Attribute-Based Encryption”, Conference on Security and Cryptography for Networks *PP.1-32.*

[2] John Bethencourt, Amit Sahai and Brent Waters, “Ciphertext-Policy Attribute-Based Encryption”,

[3] Jason Crampton, “Cryptographic Enforcement of Role-Based Access Control”, *Technology*

[4] Cheng-Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang, “A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments”, International Journal of Network Security, *Vol.15, No.4, pp. 231-240, July 2013.*

[5] Luan Ibraimi, Milan Petkovic, Svetla Nikova, Pieter Hartel and Willem Jonker, *“Mediated Ciphertext-Policy Attribute-Based Encryption and its Application”.*

[6] Natarajan Meghanathan ,"Review Of Access Control Models For Cloud Computing”, Computer Science & Information

[7] Mrs. Sunitha B.S, Dr.Anir Ban Basu," Review of Role Based Access Control Method for Securing User Space in Cloud Computing", International Journal of Computer Trends and Technology, *vol. 14 no. 1, Aug. 2014 .*

[8] S Sankareswari, S.Hemanth, "Attribute Based Encryption with Privacy Preserving using Asymmetric Key in Cloud Computing ", International Journal of Computer Science and Information Technologies, *Vol. 5 (5) , 2014, 6792-6795*

[9] K. Hemanthi, M. Sree Bala, Dr. S. Sai Satyanarayana Reddy ,"Multi Authority Attribute-Based Encryption for Securely Sharing Personal Health Records in Cloud Computing ",International Journal of Advanced Research in Computer Science and Software Engineering ,*Volume 4, Issue 7, July 2014.*

[10] Punya Peethambaran1 and Dr. Jayasudha J. S. ,"Cloud Based Access Control Model For Selective Encryption Of Documents With Traitor Detection ",International Journal of Network Security & Its Applications, *Vol.6, No.5, Sept. 2014.*