ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

DROP: Efficient and Secure Method for Cloud Data Security

Snehal Bodake[1], Prof. S. A. Kahate[2]

M.E. Student, Dept. of Computer Engineering, SPCOE, Otur, Pune, Maharashtra, India[1]

Assistant Professor, Dept. of Computer Engineering, SPCOE, Otur, Pune, Maharashtra, India[2]

ABSTRACT: Cloud storage service is one of cloud services where cloud service provider can provide storage space to customers. Because cloud storage service has many advantages which include convenience, high computation and capacity, it attracts the user to outsource data in the cloud. However, the user outsources data directly in cloud storage service that is unsafe when outsourcing data is sensitive for the user. Therefore, ciphertext-policy attribute-based encryption is a promising cryptographic solution in cloud environment, which can be drawn up for access control by the data owner to define access policy. Unfortunately, an outsourced architecture applied with the attribute-based encryption introduces many challenges in which one of the challenges is revocation. Cloud computing is an emerging computing paradigm, enabling users to remotely store their data in a server and provide services on-demand. In cloud computing cloud users and cloud services providers are almost certain to be from different trusted domain. The confidentiality of the data is major problem when users use commercial cloud servers to store their records because it can be view by everyone, by assuring that the users control the access to their own records, it is a promising method to encrypt the files before outsourcing and access control should be enforced though cryptography instead of role based access control. Cipher text-policy attribute based hybrid encryption is a promising cryptographic solution to these issues for enforcing access control policies defined by data owner on outsourced cloud data.

KEYWORDS: Cipher text-policy attribute-based hybrid encryption User revocation Dual Encryption Selective group key distribution

I. INTRODUCTION

Consumer-oriented applications such as financial portfolios, to deliver personalized information, Cloud computing means that instead of using the to provide data storage or to power large, entire computer hardware and software to be on the immersive online computer games. Often, virtualization desktop or somewhere inside the company's network, techniques are used to maximize the power of cloud it's provided as a service by another company and computing. Challenging issues are the enforcement of accessed via Internet. This is usually performed in aauthorization policies and the support of policy updates. completely seamless way. Exactly where the hardware and Ciphertext-policy attribute-based encryption [1] is a software is located and how it all works doesn't matter to proposed cryptographic solution for these issues to the user it's just somewhere up in the nebulous "cloud" enforce the access control policies that is defined by a that the Internet represents. data owner on outsourced data. The problem in applying The cloud computing goal is to apply traditional, the attribute-based encryption [2] introduces several supercomputing, or high-performance computing pointer challenges in an outsourced architecture with regard to normally used by military and research facilities, the attribute and user revocation. The study proposes an to perform tens of trillions of computations per second in, access control mechanism with a ciphertext-policy attribute-based encryption for enforcing the access attribute keys for users. It grants differential access rights control policies with many efficient attribute and user to individual users based on the attributes. It is the only revocation capability. The fine-grained access control is party that is fully trusted by all entities participating in the achieved by dual encryption mechanism. This method takes an advantage of the attribute-based encryption and data outsourcing system. selective group key distribution in each attribute group. Data Owner: This is a client who owns data and wishes

II. RELATED WORKS

Analysis is the process of breaking the problem into the successfully manageable parts of study. In system analysis emphasis is given to understanding the details of an existing system or a proposed system is desirable or not. Thus, system analysis is the process of investigating a system, identifying problems and using the information to recommend to the system. CP-ABE Methodology: The working algorithm logic in encryption is ABE comes in two types called Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). The attribute in KP-ABE, are used to describe the encrypted data [3] and policies that are built into user's keys. In CP-ABE, the attributes are used to describe a user's credential and an encryptor determines a policy on who can decrypt the data's-ABE is more appropriate to the data outsourcing architecture [4] than KP-ABE because it enables data owners to choose an access structure on attributes and to encrypt data to be outsourced under the access structure via encrypting with the corresponding public attributes.The problem occurs while applying the ABE to the data outsourcing architecture which gives challenges with regard to the attribute and user revocation. The revocation issue is difficult particularly in ABE systems, since each attribute is conceivably shared by multiple users. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. This results in bottleneck during a re-keying procedure or security degradation in the system. Thus, in this study will attempt to solve these problems in attribute-based data access control using CP-ABE for data outsourcing systems. The existing system depending full of manual process, manual system maintains the limited number of process. The existing system includes an attribute-based access control scheme using CP-ABE with efficient attribute and user revocation capability for data outsourcing systems. The existing system consists of the following entities

Trusted Authority: It is a key authority for the attributes set. It generates public and secret parameters for the system. It is in charge of issuing, revoking and updating to outsource it into the external data server provided by the service provider. A data owner is responsible for defining (attribute-based) access policy and enforcing it on its own data by encrypting the data under the policy before outsourcing it.

User: This is an entity who wants to access the outsourced data. A user possesses a set of attributes which satisfies the access policy of the encrypted data defined by the data owner and is not revoked in any of the attribute groups, then the user will be able to decrypt the ciphertext [5] and obtain the data.

Service Provider: It is an entity that provides a data outsourcing service. It consists of data servers and a data service manager. Outsourced data from data owners are stored in the data servers. The data service manager is in charge of controlling the accesses from outside users to the outsourced data in servers and providing corresponding contents services.

The following are the drawbacks of CP-ABE system are handling the outsource data copies in a secure manner is difficult. Storing and retrieving of data from a cloud server are takes more time and effort. The data owner need to take full charge of maintaining all the membership lists for each attribute group to enable the direct user revocation. All the data is maintained by single service provider so the data privacy [6] affected by the third party storage area. The single data service manager is in-charge of managing the attribute group keys per each attribute group. Key storage of each outsourced data maintenance will be difficult for the cloud administrator.

Keys are assigned randomly and independently from each other, so the user can access the data of another user group by the system.No capability to capture a series of attribute queries option.User profile is group into single group attribute in the tuples structure only. Past query based suggestion is not given to user group.

Objectives of the proposed system are to revocate users by any service provider may if unauthorized user tries to access the data above a given count. To maintain data servicing by more than one service provider. To make all data service managers take charge ofmanaging the attribute group keys per each attribute scheme also adapts a dual encryption approach togroup. To assign keys based on a condition and unique overcome the user access control problem inamong all users. attribute-based encryption system. In addition,

III. PROPOSED SYSTEM

The proposed system needs to be implements all the existing system concepts in which the Ciphertext-Policy Attribute-Based Encryption with User Revocation. The proposed scheme also adapts a dual encryption approach to overcome the user access control problem in attribute-based encryption system. Need a proposed system to allow a data owner to define the access control policy and enforce it on the outsourced data. It also enables more fine-grained access control with efficient attribute and user revocation capability [7]. The different users are allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access and to avoid these issues, there will be a need for the proposed system.

ECP-ABE- Methodology: In proposed ECP-ABE system, first, enabling user access control enhances the backward/forward secrecy of outsourced data on any membership changes in attribute groups compared to the attribute revocation [8] schemes. Second, the user access control can be done on each attribute level rather than on system level, so that more fine-grained user access control can be possible. In practical scenarios, users may miss many key update messages so that it cannot sometimes keep the key states up-to-date. This is called stateless receiver problem. In the proposed scheme, rekeying in the attribute group is done with a stateless group key distribution mechanism using a binary tree. This alleviates the scalability problem and resolves the stateless receiver problem. Third, data owners need not be concerned about any access policy for users, but just need to define only the access control policy [9] for attributes as in the previous ABE system. Objective of the proposed system is to reduce the time consuming and make the system more user friendly, efficient, accurate and fast process. The primary objective of the proposed system are to revocate users by any service provider may if unauthorized user tries to access the data above a given count. To maintain data servicing by more than one service provider. To make all data service managers take charge of managing the attribute group keys per each attribute group. To assign keys based on a condition and unique among all users. The proposed system implements all the existing system concepts in which the Ciphertext-Policy Attribute-Based Hybrid Encryption with User Revocation [10] [11] is carried out. Like existing system, the proposed multiple service providers are included and data is distributed among them. User privileges may be varying for data maintained by different service providers. This requires different kind of encryption mechanisms in data maintained by different service providers.

The advantages of proposed system are any service provider may revocate users if unauthorized user tries to access the data above a given count. Data servicing is maintained by more than one service provider, the authentication process is enhanced. All data service manager take charge of managing the attribute group keys per each attribute group. Keys are assigned based on a condition and unique among all users, so the key duplication is not occurred in the current system. Handling the outsource data copies in a secure [12] manner is easy to compare proposed attribute access control model. To capability and capture a series of attribute queries option. User profile is group into same group with attribute in the tuples structure only. Past query based suggestion is given to user group.

All the data is maintained by multiple service providers so the data privacy do not affected by the third party storage area. The single data service manager is in-charge of managing the different attribute group keys per each attribute groupCipher Text-Policy Attribute-Based Hybrid Encryption with User Revocation

Setup: The setup algorithm is executed which is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public key PK and a master key MK.

Attribute Key Generation: The attribute key generation algorithm is executed which takes input the master key MK, a set of attributes L and a set of user indices U u as parameters. It outputs a set of private attribute keys SK for each user in U that identifies with the attributes set.

Key Encrypting Key Generation: The key encrypting key (KEK) generation algorithm is executed in this module, which takes a set of user indices U as input and outputs KEKs for each user in U, which will be used to encrypt attribute group keys for each Gi.

Encrypt: An encryption algorithm (which is a randomized algorithm) that takes as input the public parameter PK, a message M and an access structure [13] 'A' over the universe of attributes. It outputs a cipher text CT suchthat only a user who possesses a set of attributes that This form is used for the purpose of that satisfies the access structure will be able to decrypt the message.

Reencrypt: The re-encryption algorithm is a randomized algorithm that takes as input the cipher text CT including an access structure 'A' and a set of attribute groups G. If the attribute groups appear in 'A', it re-encrypts CT for the attributes; else, returns ?. Specifically, it outputs a re-encrypted cipher text CT' such that only a user who possesses a set of attributes that satisfies the access structure and has a valid membership for each of them at the same time will be able to decrypt the message.

Decrypt: The decryption algorithm is executed which takes as input the cipher text CT' which contains an access structure 'A', a private key SK and a set of attribute group keys [14] for a set of attributes. The decryption can be done if satisfies 'A' and is not revoked.

Encryption and Decryption for Different Service Providers: If the data contains most important information and in order to protect the data security, more privileged service providers view most of the data and less privileged service providers view limited data.

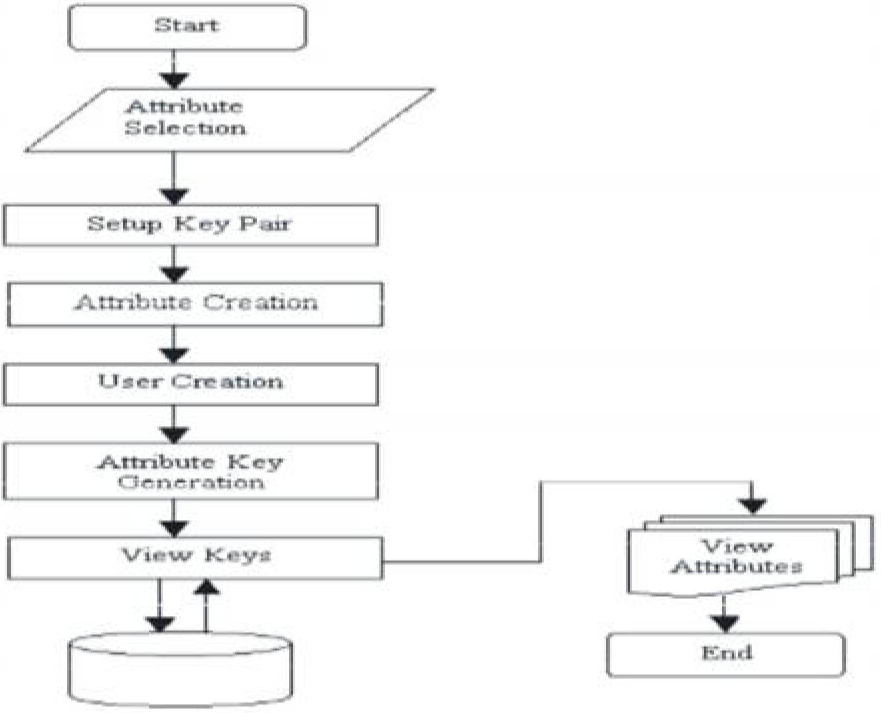

Fig. 1 System Flow

authentication with the credential details of the username and password. Those details are entered by user in the textbox controls and login process done by the command button event. Here the details are extracted from the login table for the authorization process.

Trusted Key Pair: The trusted key pair created in the application for further process, following the key generation of the public key and the master key which are used for the purpose of encryption of the message. All such keys are created as group key. These details are generated by create command button event and showed in the multiline text

Attribute Creation: This form is used to create the attribute details in the application, It contains details such as attribute id, attribute names that are entered by user in the textbox controls and saved by the save command button. The delete button is used is used to delete the specified record and close command button is user to terminate the current form.

User Creation Form: The user creation form is to create the user details for accessing the attribute with privilege level. The user id, user name and passwords are entered by user in the textbox controls these details are saved by the save command button event. The delete button is used is used to delete the specified record and close command button is user to terminate the current form.

Attribute Key Generation: Attribute key generation form is used to process the key generation process in the application. The access structure form is used to create the access specification for each and every user for specifying the details with the rights to select, insert, update and delete operation in those processes which are selected by the check box control. Attribute identity number and user identity numbers are selected by user from the ComboBox control. Given attribute name and user names are displayed in the textbox control. All these information are saved in the database using save command button event.

Attribute Group Key Generation: Attribute group key generation form is used to create group key in the application, attributes assigning with the group, identify each user belonging to the given group id. The attribute identity number

Group Keygeneration for Users: This form is used to field two and field three data's are entered by user in the
is selected by the user in the checkbox control. Group identity number is inserted in the textbox control. All these details are saved in the specified table.

DOI:10.15662/IJAREEIE.2017.0605088

assign the user to group, for accessing the given process. The user identity number is selected by user in the check box control and group identity number is selected by the combo box control and all these details are saved in the specified Table.

Key Encrypting Key Generation for Users: This form is used to encrypt the key value for corresponding username and user id. The id details are selected by user in the checkbox control and user key is generated using create command button event. The corresponding username, user id and the given key encrypting values are inserted into the user details table.

Encryption Form: This form is used to encrypt the text using public key for the purpose of other users who do not know the given message. So, the public key is extracted using get key command button and displayed in the label control, the message is entered in the textbox control then the given encrypted message is displayed in the label control. The encrypted message is saved in the application using creates cipher text and save command button event.

Re-Encrypt Form: This form, re-encrypt the encrypted data in the application based on the group key because the other user will not identify the same encrypted message. In this form, group identity number and cipher texts are selected from the combo box controls and details are re-encrypted in the cipher text grid view control using re-encrypt command button event.

Decrypt Cipher Text: Decrypt cipher text retrieves the plain data in the application. The given cipher text is entered the data is showed to the user. In this form user identity number and cipher texts are selected from the combo box control, group identity is displayed in the label controls. The message is decrypted in the cipher text grid view control using the decrypt command button event.

Select Query Form: This form is used to check the user level access privileged rights in the application; query is inserted in the textbox control and processed by the check command button event.

Encrypt Block Security Form: This form is used to create cipher text in this experimental system given database the user access the high privileged level or not. The field one, list box controls and privilege settings is selected by the check box control. The Advanced Encryption Key (AES) is entered in the textbox control and data is encrypted using the encrypt command button event.

IV. CONCLUSION

The rapid development of versatile cloud services, a lot of new challenges have emerged. One of the most important problems is how to securely delete the outsourced data stored in the cloud severs. The proposed ciphertext-policy attribute-based hybrid encryption with user revocation scheme provides a big advantage by supporting user-defined time-specific authorization and fine-grained access control and data secure self-destruction. Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. This thesis proposes a cryptographic approach to enforce a fine-grained access control on the outsourced data that is dual encryption protocol exploiting the combined features of the ciphertext-policy attribute-based hybrid encryption and group key management algorithm. The proposed scheme allows a data owner to define the access control policy and enforce it on his outsourced data. It also features a mechanism that enables more fine-grained access control with efficient attribute and user revocation capability. It is sent that the proposed scheme is efficient and scalable to securely manage the outsourced data. The proposed ciphertext-policy attribute-based hybrid encryption model does includes the set of the attributes, tree access policy and the definition of the time instant, because the costs are negligible if compared with the key generation.

Future Enhancement: The proposed ciphertext-policy attribute-based hybrid encryption with user revocation supports the function of user-defined authorization period and ensures that the sensitive data cannot be read both before its desired release time and after its expiration. In future the authorization period can be incorporated with the user session of the cloud server to provide the improved security mechanism.

REFERENCES

1. Ibraimi, L., M. Petkovic, S. Nikova, P. Hartel and W. Jonker, 2009. “Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application,”Proc. Int’l Workshop Information Security Applications (WISA ’09), pp: 309-323.
2. Sahai, A. and B. Waters, 2005. “Fuzzy Identity-Based 9. Vimercati, S.D.C., S. Foresti, S. Jajodia, S. Paraboschi Encryption,” Proc. Eurocrypt ’, 05: 457-473. and P. Samarati, 2007. “Over-Encryption: Goyal, V., O. Pandey, A. Sahai and B. Waters, 2006.
3. Management of Access Control Evolution on “Attribute-Based Encryption for Fine-G Outsourc Data,” Proc. Int’l Conf. Very Large Data Access Control of Encrypted Data,” Proc. ACM Bases (VLDB ’07). Conf. Computer and Comm. Security, pp: 89-98.
4. Naor, D., M. Naor and J. Lotspiech, Vimercati, S., S. Foresti, S. Jajodia, S. Paraboschi and “Revocation and Tracing Schemes for Stateless P. Samarati, 2007. “A Data Outsourcing Architecture Receivers,” CRYPTO’01: Proc. Int’l Cryptology Conf. Combining Cryptography and Access Control,” Proc. Advances in Cryptology, pp: 41-62. ACM Workshop Computer Security Architecture

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

5. Liang, X., R. Lu, X. Lin and X. Shen, (CSAW '07), Nov. 2007. "Ciphertext Policy Attribute Based Encryption with Bethencourt, J., A. Sahai and B. Waters, 2007. Efficient Revocation," technical report, Univ. of "Ciphertext-Policy Attribute-Based Encryption http://bbcr.uwaterloo.ca/~x27liang/papers/ Proc. IEEE Symp. Security and Privacy, pp: 321-334.
6. Baden, R., A. Bender, N. Spring, B. Bhattacharjee and 12. Pirretti, M., P. Traynor, P. McDaniel and B. Waters, D. Starin, 2009. "Persona: An Online Social Network 2006 . "Secure Attribute-Based Systems," Proc. ACM with User-Defined Privacy," Proc. ACM SIGCOMM Conf. Computer and Comm. Security. '09, Aug. 2009.
7. Ostrovsky, R., A. Sahai and B. Waters, 2007. Boldyreva, A., V. Goyal and V. Kumar, 2008. "Attribute-Based Encryption with Non-Monotonic "Identity-Based Encryption with Efficient Acces Structures," Proc. ACM Conf. Computer and Revocation," Proc. ACM Conf. Computer and Comm.Comm. Security, pp: 195-203.