International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 1| ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT19518

Improvement of Privacy and Security in Hybrid Cloud with Attribute Group Based Access Control

Kayalvili S[1], Sowmitha V[2]
[1]Computer Science and Engineering, Velalar College of Engineering and Technology,Erode, Tamilnadu, India
[2]ME-CSE, Velalar College of Engineering and Technology, Erode, Tamilnadu, India

ABSTRACT

Cloud computing enables users to accumulate their sensitive data into cloud service providers to achieve scalable services on-demand. Outstanding security requirements arising from this means of data storage and management include data security and privacy. Attribute-based Encryption (ABE) is an efficient encryption system with fine-grained access control for encrypting out-sourced data in cloud computing. Since data outsourcing systems require flexible access control approach Problems arises when sharing confidential corporate data in cloud computing. User-Identity needs to be managed globally and access policies can be defined by several authorities. Data is dual encrypted for more security and to maintain De-Centralization in Multi-Authority environment.

Keywords:ABE-Attribute Based Encryption, Authority, Fine Grained, Outsourcing, Dual Encryption.

I. INTRODUCTION

Cloud computing is internet-based computing during whichmassiveteams of remote serverssquare measure networked to permit sharing of data-processing tasks, centralized information storage, and on-line access to pc services or resources. Clouds are often classified as public, personal or hybrid. Cloud computing that depends on sharing computing resources instead of having native servers or personal devices to handle applications. The mostsanctioning technology for cloud computing is virtualization. In basic ABE systems, the data shared is oftenat intervals one domain or organization. However, in reality, infolikes drivers' licenses andregistration info in universities area unit organized by totally different government departments. The management of attributes and key distributions can't be undertaken by an equivalent attribute authority. Moreover, access methodscould also be distributed supported attributes of various authorities.

Cloud computing provides the tools and technologies to create data/compute intensive parallel applications with far morereasonablecosts compared to ancient parallel computing techniques. In Single-authority ABE, every user's keys area unit generated victimizationtotally different random and on the QT shared values specified keys generated for various users can't be combined, that prevents collusion attacks.

The main objective of this paper isn't to use a central authority to manage users and keys, and solelystraightforward trust relations have to be compelled to be fashioned by sharing the general public key between every attribute authority (AA). User identities square measuredistinctive by combining a user's identity with the identity of the AA wherever the user is found. Once a key request has to be created to associate authority outside the domain, the request has to be performed by the authority within the current domain instead of by

the users, so, user identities staypersonal to the AA outside the domain, which is able to enhance privacy and security. Here, once the user ought to requests associate attribute secret key, if the attributes square measuresituated outside the domain, the request by the supply AA within the domain to the target AA is employedinstead of by requests by users themselves.

II. RELATED WORKS

A. AData Outsourcing Architecture Combining Cryptography and Access Control

The recent adoption and diffusion of the information out-sourcing paradigm, whereverknowledge house owners store their knowledge on external servers, there are increasing general demands and issues for knowledge confidentiality. Besides well-known risks of confidentiality and privacy breaks, threats to out-sourced knowledgeembody improper use of information: the server may use substantial components of a setof knowledge gathered and arranged by the information owner, doubtless harming the information owner's marketplace for any professional duct or service that comes with that assortmentof data. The projected novel access management model and design that eliminates the necessity for a reference monitor and depends on cryptography to make sure confidentiality of knowledgehold on a server. Knowledgearea unit encrypted because theknowledge owner stores them on associate in nursing external server. Authorizations and codingarea unitunitedthereforepermitting access managementsocial control to be outsourced besidethe information. The nice advantage is that the information owner, whereas specifying the policy, wants not b econcerned in its social control.

B. Persona: An Online Social Networkwith User-Defined Privacy

These network help users share in order with their friends. However, users entrust thesocial network provider with such personal information as sexual preferences, supporting and religious views, phone numbers, occupations, identities of friends, and photographs. Although sites over privacy controls that let users restrict how their data is viewed by other users, sites provide inadequate controls to restrict data sharing with shared affiants or application developers.

C. Fuzzy Identity-Based Encryption

In this paper, discussed the use fullness of using biometric s in Identity-Based and then discuss their contributions. Using biometrics in Identity- Based Encryption in many situations, using biometric–based individuality in an IBE system has a number of important advantages over “standard” IBE. In standard Identity-Based Encryption scheme a user with a positive identity, for example, “Bob Smith”, will need to go to an authority to obtain the private key corresponding to the identity. In that process the user will need to “prove” to the authority that he is indeed entitled to this identity. That will typically involve presenting supplementary documents or credentials. Typically, there exists a trade-off between a system that is expensive in this step and one that is less reliable.

D. Mediated Cipher text-Policy Attribute-Based Encryption and Its Application

Distributed data systems needversatile access management models thattranscend discretionary, necessary and role-based access management. On the opposite hand, the present trend of service-based data systems and storage outsourcing needenhanced protection of knowledgetogether with access

managementways that area unit cryptographically implemented. The conception of Attribute-Based coding (ABE) fulfills the samenecessities. It provides a chicmanner of encrypting knowledgesuch the encryptor defines the attribute set that the decryptorhas topossesso as to decrypt the cipher-text. . A secret key holder willdecipher the cipher text if the attributes related to his secret key satisfy the access policy related to the cipher text. In these schemes, a ciphertext is related toassociate in nursing access policy and therefore the user secret keysrelated toa collection of attributes.

III. METHODOLOGY

1. EXISTING WORK

When the system is set up, the public key of each AA and the basic parameters are distributed, which simplifies the process of trust establishment. The key issuing protocol for privacy only needs to use the public key of AA to realize the trust between AA. Present data outsourcing systems require supple access control approaches. In many cases, it is attractive to provide differentiate access services such that data access policy are defined over user attributes or roles. Some of the most difficult issues in data outsourcing scenario are the enforcement of union policies and the support of policy updates. Cipher text-policy attribute-based encryption is a hopeful cryptographic solution to these issues for enforces access control policies defined by a data owner on outsourced information.

But, the problem of applying the attribute-based encryption in an outsourced architecture introduces several challenges with regard to the attribute and user revocation. So the project also proposes an access control mechanism using cipher text-policy attribute-based encryption to enforce right to use control policies with well-organized element and user revocation capability. The fine-grained way in control can be achieved by dual encryption method which takes advantage of the attribute-based encryption and discerning group key distribution in each attribute group. This work demonstrates how to apply the proposed mechanism to securely manage the outsourced data. The analysis results point to that the proposed system is efficient and protected in the data outsourcing systems.

The concept of attribute-based encryption (ABE) is a promising approach that fulfills these requirements. ABE features a device that enables an entrance control over encrypted data using access policies and qualified attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryption defines the attribute set that the decryptor needs to have classify to decrypt the cipher text.

2. PROPOSED WORK

- Attribute Group - Based Encryption is managed. It adapts a dual encryption approach to overcome the user access control problem.
- Multiple attribute groups are included and data is distributed among them. User privileges may be varying for data maintained by different attribute groups.
- The data owner maintains all the membership lists to enable the direct user management in more than one place.
- Keys are assigned randomly and independently from each other. But group key mechanism is common for users in single group
- All the data is maintained by more authority groups.

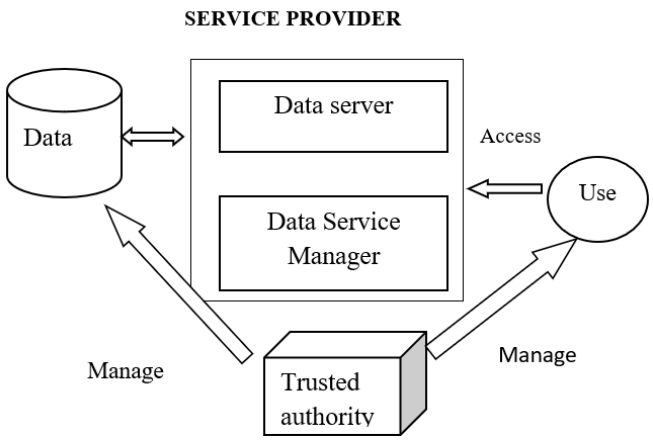

Fig 1.1. Privacy and Security Improvement

a) Trusted Key Pair

The trusted key pair created in the application for further process, following key generate the public key and master key, for the purpose of encrypt the message and group key is created. These information are generate by form command button event and showed in the multiline text mode. These key saved in the relevance using save authority key event.

b) Attribute Creation

It contains details such as attribute id, attribute names 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 specific record and close command button is user to terminate the current modules.

c) User Creation

Used to create the client facts for accessing the attribute with privilege level. The client id, user first name and passwords are enter by user in the textbox control these details are saved by the save command button event. The delete button is used is used to delete the specific record and close command button is user to terminate the current modules.

d) Attribute Key Generation

This module is used to process the key generation process and the access structure modules is used to create the access specification for each and every user for specifying the details with the rights of select, insert, update, delete operation those process is selected by the check box control, attribute identity number and user identity numbers are selected by user from the Combo Box control.

e) Encryption

Encrypt the text using public key for the purpose of other users not knows the given message. So, the unrestricted key is extract using get key grasp button and displayed in the label control, the message is entered in the textbox manage then the given encrypted communication is display in the label control. The encrypted message saved in the application using creates cipher text and save command button event.

f) Decrypt Cipher Text

It is used to retrieve the plain data in the application. The specified cipher text is entered the data is showed to the user. In these module user characteristics number and nobody texts are selected from the combo box control, group identity is display in the label controls. The significance is decrypted in the cipher text grid view control using the decrypt authority button occurrence.

The following Table describes experimental result for proposed system secure attribute selection analysis. The table contains number of time slot interval and given attribute to calculate average numbers of selection attribute details are shown.

Member Node	Existing System (%)	Proposed System (%)
8	72.54	78.62
12	76.13	78.11
16	82.42	83.13
24	86.66	84.67
30	88.13	89.78
32	80.44	82.66
38	78.33	80.21
42	87.22	89.76
46	79.22	80.65

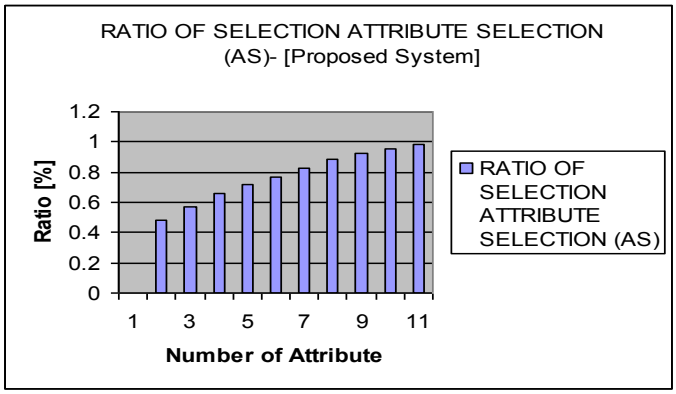

Fig 1.2 Attribute selection- Ratio Analysis

IV. CIPHER TEXT-POLICY ATTRIBUTE-BASED ENCRYPTION

STEP 1:

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

STEP 2:

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

STEP 3:

The key encrypting key (KEK) generation algorithm is executed in this module, which takes a set of user indices $U \subseteq u$ as input, and outputs KEKs for each user in U, which will be used to encrypt attribute group keys $K_{\lambda i}$ for each $Gi \in G$.

.

VII. CONCLUSION

- Authorization policies and the support of policy updates are studied.
- Proposes a cryptographic approach for communication between users and attribute authorities.
- Allows a data owner to define the access control policy and enforce it on his outsourced data.
- Efficient and scalable to securely manage the outsourced data.

VIII. FUTURE WORK

- It allows a data possessor to define the access control guidelines and enforce it on his outsourced data.
- It also features a method that enables more fine-grained access control with efficient attribute and user revocation capability. The proposed scheme will be efficient and scalable to firmly manage the outsourced data.
- The innovative system is designed such that that enhancement can be integrated with current modules easily with less integration work.

IX. REFERENCES

[1]. S. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "A Data Outsourcing Architecture Combining Cryptography and Access Control," Proc. ACM Workshop Computer Security Architec-ture (CSAW '07), Nov. 2007.

[2]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009.

[3]. R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin,"Persona: An Online Social Network with User-Defined Privacy,"Proc. ACM SIGCOMM '09, Aug. 2009.

[4]. A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc.Eurocrypt '05, pp. 457-473, 2005.

[5]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[6]. J. Anderson. Computer security planning study.Technical Rep ort 73-51, Air Force Electronic System Division, 1972.

[7]. J. Saltzer and M. Schro eder. The protection of information in computer systems. Communications of the ACM , 17(7), July 1974.

[8]. N. Provos . Encrypting virtual memory. In Proc. of the 9th USENIX Security Symposium , Denver, Colorado, USA, August 2000.

[9]. A. Harrington and C. Jensen. Cryptographic access control in a distributed ¯le system. In Proc. of the 8th SACMAT , Como, Italy, June 2003.

[10]. S. Akl and P. Taylor. Cryptographic solution to a problem of access control in a hierarchy. ACM TOCS , 1(3):239{248, August 1983. Germany, Septemb er 2007.

[11]. J. Crampton, K. Martin, and P. Wild. On key assignment for hierarchical access control. In Proc. of the 19th IEEE CSFW'06 , Venice, Italy, July 2006.

[12]. G. Miklau and D. Suciu. Controlling access to published data using cryptography. In Proc. of the 29th VLDB Conference , Berlin, Germany, Septemb er 2003.

[13]. H. Hacig Aum Aus, B. Iyer, and S. Mehrotra. Providing database as a service. In Proc. of 18th ICDE , San Jose, CA, USA, February 2002.

Cite this article as :

Kayalvili S, Sowmitha V, "Improvement of Privacy and Security in Hybrid Cloud with Attribute Group Based Access Control", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 57-61, January-February 2019.

Available at doi :

https://doi.org/10.32628/CSEIT19518

Journal URL :http://ijsrcseit.com/CSEIT19518