Combination of Role Based Access Control and Hierarchical Identity Based Re-Encryption for Secure Data Recovery

M. Kowsalya
M.E Computer Science and Engineering, Sona College of Technology, Salem.

Abstract - Unauthorized users may access the data stored in cloud due to its vulnerability in control over security system. This may lead to leakage of information which in turn ruinsuser's privacy .In order to provide solutions to these problems we need to provide ultimate protection of resources in terms of storage and retrieval. Cloud users usually prefer to minimal searching time to find appropriate data. In existing system they use keyword approach and it will not detect inconsistencies and data leaks .Cipher Text Attribute Based Encryption algorithm is used for authentication mechanism which will not support key leakage in user's application. We propose Key Policy Attribute Based Encryption approach to have a combination of Role Based Access Control Mechanism (RBAC) and Hierarchical Identity Based Re-encryption (HIBR) to reduce the risks of data loss and maintain them by only giving access permission in their level of authority.

Keywords: Access Rights, Attributes, Secret code, Authentication, Multikeyword search.

I. INTRODUCTION

Cloud Storage is appropriate for storing data with multi keyword that requires low latency access or data that is frequently accessed based on searching pattern over encrypted data such as serving website content, interactive workloads, or data supporting mobile and gaming applications. In Cloud we usually upload or store the data. Once storage is over, your data will be replicated in multiple data centre, so that the data will be available based on their needs and also reduce your bandwidth usage. Thus users can predominately access them anywhere. Here comes, the challenge of access rights to users who may be unauthorized person, attacker or normal cloud users. In order to protect the data or to distinguish them with their access rights, each users have given access rights based on their hierarchy level to their position, which is similar to patients records in a hospital such as nurse can categories the records of patients, doctors can make modifications regarding treatments, patients relatives can only view the records .Role based access control mechanism based on Hierarchical Identity Based Re-encryption which gives a solution to users who can access them only when he is an authorized person.

II. RELATED WORK

N. Cao [2] propose some issues in Privacy preserving multi keyword ranked search which is burden of sorting through every match in content selection in terms of outsourcing complex data management systems from local sites to commercial public cloud. No search control or access control is initiated in coordinate matching and inner product similarity .Communication cost is based on retrieval of documents and also overhead occurs in association between keyword and encrypted documents

CengizOrencik [4]stated that private information retrieval needs cryptographic tools to hide important documents to cloud users and searching terms by query process.Symmetric key which can be used as trapdoor for authenticated users.It is not applicable because users must know all valid keywords and their level of position to generate the query.

Rani.A [12] address challenges in transferring the data secretly and its major drawback is to handle key generation centre which transport all keys leads to data leakage.Threats may occur in case of improper use of data by storage server and unauthorized access by outside users.Users privacy depend on honest behaviour of attributes usage.

MeenaKowshalya.A [10] study modified escrow free key generation protocol come with solution that data owners may update their change and policies in attributes but has overhead in rekeying and message for user update.The useralso needs to contact both data storing centre and key generation centre

Aparna.V[1] define that Mediated cipher text Attribute Based Encryption needs natural language processing algorithm for identifying attributes in content selection and user has to update their private key regularly .Thus it leads to scalability issues. Moreover user should define their attributes and create their own key.

Saroja.D[13] Cloud users usually store their data with secure password such as one of their personal details. Escrow problem provides solution in two ways such as

cipher text and Key policies Attribute Based Encryption. In which attribute keys are distributed based on their pattern in which selection is made. These attribute keys placed in a group using CPABE. Only using Membership management and user revocation ,keys are decrypted to other users. Separate data storing center is needed for all keys. But the problem arises such as access policy in decision making, security threats includes data secrecy, complicity conflict, updating should be made then and there , disjoint attribute authorities and it decreases the performance. Most difficult one is user can encrypt their data and upload them only once.

Kalaiselvi.M[6] In this technique matrix type key generation , users they themselves specify attribute for encryption and also algorithm for encrypting their message and at last keys are generated with the algorithm without the intervention of the users. Using Hierarchical method the importance of each data is analyzed with the authority who is seeking them based on higher priority and lower priority. In this method selection of key is done among application center, key generation center, data storing center. So users should double encrypt each data for storing and retrieving them. Hypervised techniques is time consuming process. Especially using different algorithm, it has drawbacks in network traffic, time complexity and also every user's specification differs. In authentication process, admin act as a interface between user and system. Data encryption and re-encryption is also done by data owner and it is then transferred to data storing center and using partial disclosure algorithm data is retrieved based on hierararchy.

Praveen Kumar.C[11] Cost effective data transmission highlights some of the importance in avoiding certificate verification which is the way to save communication and computation workloads. Energy usage of data basically in smart grid is only for efficiently using them. They used ring signature for anonymous authentication while sharing the data.Fine grained mechanism is used for uploading the data. This method is used only when it ensures the data availability and access control over them to provide protection by signature. In a group any one of the member is compromised , their previous authentication is still protected. But the problem lies with private key generation which is done by key generator, data owner should keep their secret key efficiently and cloud provider should provide secure access control to the users.

III. MULTIKEYWORD SEARCH

Cloud users outsource the data to external cloud servers for scalability in storing data. Whenever we need to transfer the data there occurs security concerns in terms of secrecy.

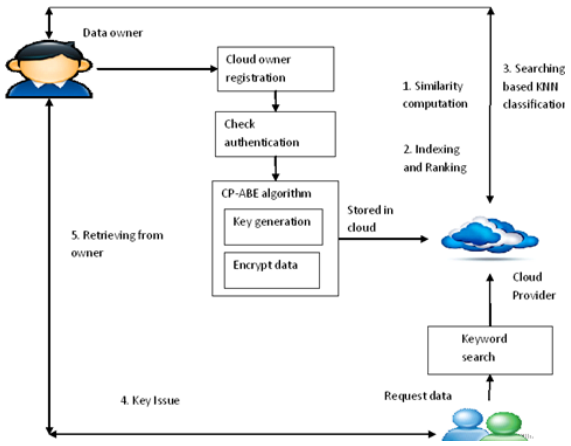

Figure 3.1 Retrieval of Encrypted Information

One of the issue in retrieving the encrypted cloud data is to deliver the accurate information. This can be done using multi keyword ranked search and also reduce the searching time. Searching can be done using relevance score and k – nearest neighbor techniques to improve the efficiency for huge amount of outsourced documents in cloud. Identifying the appropriate files through multi keyword search made by indexing and ranking pattern. Moreover it has adopted the blind storage system in which access pattern is always in hidden manner. Thus it provides confidentiality of documents and indexing, trapdoor privacy, trapdoor unlink ability.

IV. ACCESS BY AUTHENTICATION

The data like personal details in an organization, secret information/secret code in their private sectors are shared among themselves and distributed over cloud.

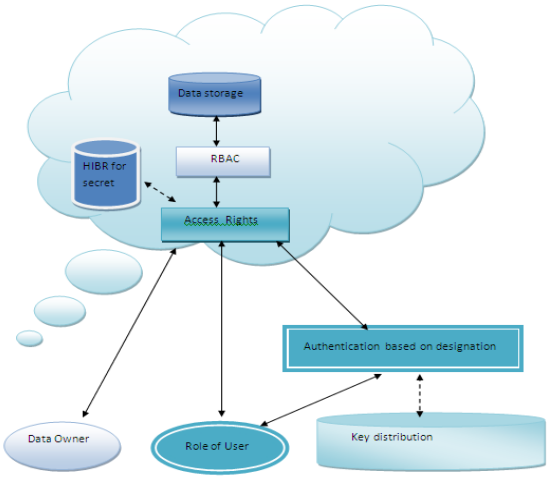

Figure 4.1 Access permission for Retrieval

Their encryption is done based on content selection with their secret code of using attributes. It usually distribute data at coarse-grained level(i.e. your secret code is used by another user).Instead of using coarse grained level of sharing , we choose fine tuning of access which we call it

as Key-Policy Attribute Based Encryption(KP-ABE).In this cryptosystem, keys are labelled with specific set of attributes and their secret key for association. Thus access rights is framed with designation (i.e. level of authority) to ensure that he or she belong to trusted users. We propose an approach, Role based access control mechanism supports HIBR for categorizing their users position and accessing role which is measured through audit log information and broadcast re-encryption.

Role Based Access Control Mechanism

It gives neutral access control to the user based on their position. Similary one to one correspondence is assigned to the cloud users which is as following role->users, authority, access control based on the permission it seeks.The priviledge possessed by each user is done by relationships(one-one, one- many, many-many).Thus the security crisis in cloud is facilitated by huge number of users and so their complications can be eradicated by restricted policies and procedures.Roles are created for various access controls which gains several advantages over operations such as add, delete and modify them.

- USERS, Authority(Doctors,patient, nurse), FUN(add, delete, update), and S (authority->authorisation).
- AU Authority,Users, a many-to-many mapping authority-to-users relation.
- authorized users: (r:authority) $\rightarrow$2^authorized users, the mapping of authority r onto a set of authorized users. Formally: authorized_users(r) = {u ε authority (u, r) ε AU}.
- AC= 2 ^ (FUN, S), the set of access control.
- AC $\subseteq$ Authority x access rights, a many-to-many mapping access control to access rights relation.
- Access rights(r: user access) $\rightarrow$ 2^authority, the mapping of user access r onto a set of access rights. Formally: access rights(r) = {u ε access rights (ac r) ε AC}.
- S(AC: access rights) $\rightarrow${f $\subseteq$ FUN}, the access rights to-function mapping, which gives the set of functions associated with access rights.
- S(AC: access rights) $\rightarrow$ {s $\subseteq$ S}, the access rights-to-security mapping, which give the set of secure access associated with access rights.
- SESSIONS, the set of sessions.
- Authorized user sessions (Au: USERS) $\rightarrow$ 2^SESSIONS, the mapping of authorized user u onto a set of sessions.
- session authority (s: SESSIONS) $\rightarrow$ 2^authority, the mapping of session s onto a set of authority. Formally: session authority (sa) $\subseteq$ {r ε authority | (session_authority (sa), r ε AU}.

Hierarchical Identity Based Encryption

Once the role is assigned,the next process is to verify them. Verfication possess selection in which it requires identification(User-ID) for restricted secret key access.It periodically verifies for changes that has been made.Thus changes doesnot affects the storage of data which is replicated in multiple sites.It is of tree based access structure that gives authorization

- **Authorized user identity UD:** Assinging users according to their position,such as UDs: (UD1*; : : : ;* UD*l*).Higher authority in the hierarchy tree are the root SK(secret key)and the users lower authority SK
- **Hierarchical Identity-Based Encryption (HIDE):** a HIDE scheme is split into five properties
- randomized algorithms: Higher authority, priority level, Access given, Encryption, and Decryption:
- **Higher Authority:** The root SK takes a secure access params *S* and it includes Access rights.. The parameters include a information I and the key *K*.
- **Priority level Setup:** Each user must obtain the system parameters of the root SK.priority level is based on position they acquire and constraint requires their role to limited access by issuing secret key.
- **Access Given:** A SK (higher authority to lower authority) with UD (UD1*; : : : ;* UD*l*) may acquire a secret key for any of its position(A) such as , UD (UD1*; : : : ;* UD*l;* UD*l*+1),UD+Ai) by using the system parameters and its secret key .
- **Encryption:** A sender sends input as I+E(Encrypted key) as parameters and purposeful information and computes its value
- **Decryption:** A user inputs *params*, *I+D(Decrypted key)*, and its secret key *s*, and returns the message V(Valid) or IV(invalid)

V. KEY DISTRIBUTION FRAMEWORK

In key Distribution process multi data users (eg. Doctor, nurse, assistant doctors, patients) based on their designation can have their access rights to support anonymous authentication. The user is authenticated using attributes that are issued by data owner.

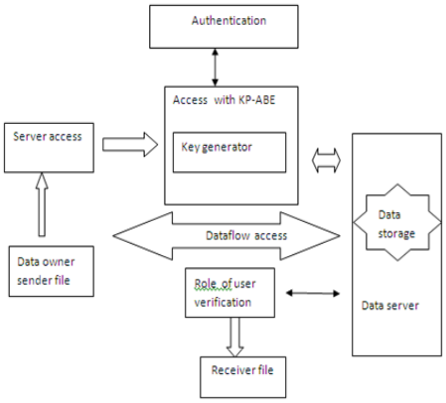

Figure 5.1 Key authentication processes

The Key authentication is flexible for data flow access, replay attacks and using KP-ABE for authentication purpose; ABE is the one of the several cryptographic algorithms, which often used to verify file based attributes also implement attribute based access control whereby access privileges are granted to users during the use of their role which merge attributes together for providing secret code

Steps for Key Process

In the first process cloud admin verifies cloud users by authorization procedure in terms of key access using RBAC and HIBE for maintaining the data protection.Secondly it finds the authority of users needs by their position based on the access by verification.Finally secret key given to the cloud user to retrieve the data.

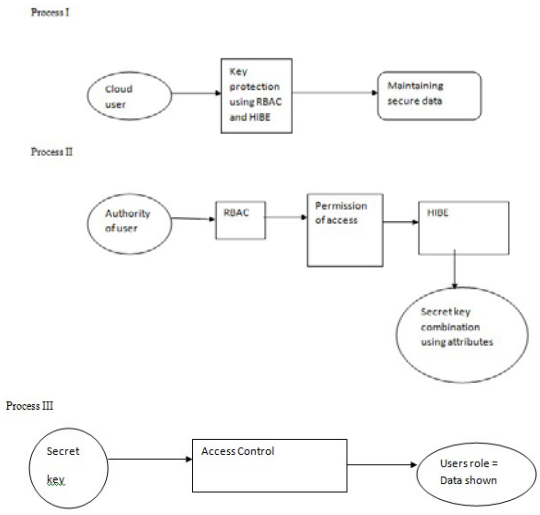

Figure 5.2 Process of key access

Sample of Execution

Figure 5.3 shows the role of each user and their requirements will be established.

Figure 5.3 Role Access

Figure 5.4 shows keyword search for more specific details it consumes for access

Figure 5.4. Keyword Search

Figure 5.5 shows the unique details of User-ID it possess with security

Figure 5.5 Access Information

The Secret code can use any type of attributes (user attributes, resource attributes, environment attribute etc.). Accordingly, RBAC with HIBR supports user authentication before information retrieval. In this approach, access is granted to the user based on their designation followed by their secret code such as barcode reader. We can implement this process in real time cloud environment and improve accuracy.

VI. EXPERIMENTAL RESULTS

We can simulate the performance of the system by using the parameters such as (i) increasing the keyword search in search process,(ii) increasing the number of access permission based on designation,(iii) increasing the user attributes,(iv) These evaluation is done in terms of storage overhead, computational efficiency and communication cost.

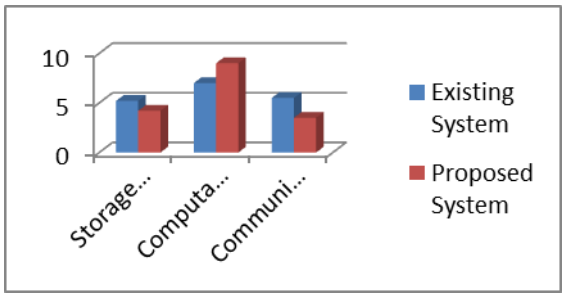

Figure 6.1 Simulation result

VII. CONCLUSION

In this paper, we contribute access control mechanism for delegate authentication. Security is the major concern for sensitive data. Secret Key should be maintained by monitoring their role of access to choose which information the user can view or to share over network. Thus RBAC with HIBR supports authorization of users by validating their attributes to ensure that the data is accessed only by legitimate users and then user can receive required information.In future work, we can implement double encryption system to encrypt and decrypt the data double time. Using mediated certificate less public key encryption (mCL-PKE) scheme, we can build the solution to the problem of sharing sensitive information in public clouds and propose an extension to improve the efficiency of encryption at the data owner.

REFERENCES

[1] Aparna.V, JabishaArul, Nandhini. S, andVishnuKumar.A,"Multi Attribute Based Technique in Key Generation System", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 –8958, Volume-2, Issue-4, April 2013.

[2] N. Cao, C. Wang, and M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," *Proc. IEEE INFOCOM*, pp. 829-837, Apr, 2011.

[3] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rou, and M. Steiner ``Highly-scalable searchable symmetric encryption with support for Boolean queries," in Proc. CRYPTO, 2013, pp. 353-373.

[4] CengizOrencik, and ErkaySavas"Efficient and Secure Ranked Multi-Keyword Search on Encrypted Cloud Data" ACM 978-1-4503-1143-4/12/03 March 30, 2012, Berlin, Germany.

[5] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, ``A survey of mobile cloud computing: Architecture, applications, and approaches," WirelessCommun. Mobile Comput. vol. 13, no. 18, pp. 1587-1611, Dec. 2013.

[6] M.Kalaiselvi,T.Amitha,"Hypervised Technique in Multi posture attribute based key generation", in International Journal of Advanced Computer Technology,vol.2,no. 2 ISSN: 2319-7900.pg. 65-71.

[7] H. Li, Y. Dai, L. Tian, and H. Yang, ``Identity-based authentication for cloud computing," in Cloud Computing. Berlin, Germany: Springer-Verlag, 2009, pp. 157-166.

[8] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, ``An SMDP-based service model for inter domain resource allocation in mobile cloud networks," IEEE Trans. Veh. Technol., vol. 61, no. 5, pp. 2222-2232, Jun. 2012.

[9] M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 10, pp. 1805-1818, Oct. 2012.

[10] A.MeenaKowshalya, and Dr.M.L.Valarmathi, Secure and Efficient Ciphertext Policy Attribute Based Encryption without key Escrow Problem", International Journal of Emerging Engineering Research and Technology Volume 2, Issue 2, PP 126-130, May 2014.

[11] C.Praveen Kumar,P.Suman Prakash,S.Prem Kumar,"Cost-Effective Authentic and Anonymous Data Sharing with Forward Security" International Journal of Computer Engineering In Research Trends(IJCERT) ISSN:2349-7084,vol. 2,pp 1126-1131,Dec 2015.

[12]Rani.A "Improving Security and Efficiency in Distributed Data Sharing and Data Leakage Detection System" International Journal of Engineering Science & Research Technology (IJESRT) ISSN: 2277-9655, Nov 2013.

[13] D.Saroja, P.Lakshmi, "Removal of Escrow Problem and Revocation Problem in Distributed Data Sharing",International Journal of Innovative Research in Computer and Communication Engineering(IJIRCCE) ISSN:2320-9801, vol.2,Sep 2014.

[14] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Y. Luo, ``Exploiting geo-distributed clouds for a e-health monitoring system with minimum service delay and privacy preservation," IEEE J. Biomed. Health Inform. vol. 18 no. 2, pp. 430-439, Mar. 2014.

[15] E. Stefanov, C. Papamanthou, and E. Shi, ``Practical dynamic searchable encryption with small leakage," in Proc. NDSS, Feb. 2014.

[16] W. Sun, et al., ``Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. 8th ACM SIGSAC Symp.Inf., Comput.Commun.Secur. 2013, pp. 71-82.

[17] B.Wang, S.Yu, W. Lou, andY. T. Hou, ``Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in Proc. IEEE INFOCOM, Apr./May 2014, pp. 2112 - 2120.

[15] Y. Yang, H. Li, W. Liu, H. Yang, and M. Wen, ``Secure dynamic searchable symmetric encryption with constant document update cost," in Proc.GLOBECOM, Anaheim, CA, USA, 2014.