RESEARCH ARTICLE OPEN ACCESS

The Recent Trend: Vigorous unidentified validation access control system with Decentralization Concept in Clouds

Y.Hymavathi [1] ,CH.Samson[2],B. Satyanarayana Reddy[3] Dr. B. Tarakeswara Rao[4]
[1] PG Student,Dept of CSE,Kallam Haranadhareddy Inst of Technology,NH-5 Guntur(dt),A.P.
[2]Assoc.Professor, Dept of CSE,Kallam Haranadhareddy Inst of Technology,NH-5 Guntur(dt),A.P
[3]Assoc.Professor,HOD, Dept of CSE,Kallam Haranadhareddy Inst of Technology,NH-5 Guntur(dt),A.P
[4]Professor,Dept of CSE,Kallam Haranadhareddy Inst of Technology,NH-5 Guntur(dt),A.P

ABSTRACT
Service Providers can grow their business by selling our cloud authentication service that can be fully branded to the Service Provider or if required a Service. The proposed enhanced decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. The scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. It addresses user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, hiding attributes, increasing high security in access, computation, and storage overheads are comparable to centralized approaches.
In Existing, it is based on ABE (attribute based encryption) technique which is a centralized approach, where a single Key Distribution Centre (KDC) distributes secret keys and attributes to all users using asymmetric key approach. We propose a new decentralized access control method for storing data by providing security in clouds and also we hide the attributes and access rule of a user. The cloud validates the authentication of the sequence without knowing the users characteristics previous to the data store. By using this approach only certified users have right to use the suitable attributes. In future, time based file revocation scheme can be used to assure the deletion of a file. When time limit of a file expires, we implement the policy based renewal of time to that file.
Key Words: Data security, Key policy ABE, Cipher Text policy ABE, Key management, cloud computing, secret key.

I. INTRODUCTION

Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents or even personal information (as in social networking). There are broadly three types of access control: User Based Access Control (UBAC), Role Based Access Control (RBAC), and Attribute Based Access Control (ABAC). In UBAC, the access control list (ACL) contains the list of users who are authorized to access data. This is not feasible in clouds where there are many users. In RBAC, users are classified based on their individual roles. Data can be accessed by users who have matching roles. The roles are defined by the system.

We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.Service Providers can grow their business by selling our cloud authentication service that can be fully branded to the Service Provider or if required a Service. The proposed enhanced decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. The scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading

data stored in the cloud. It addresses user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, hiding attributes, increasing high security in access, computation, and storage overheads are comparable to centralized approaches.

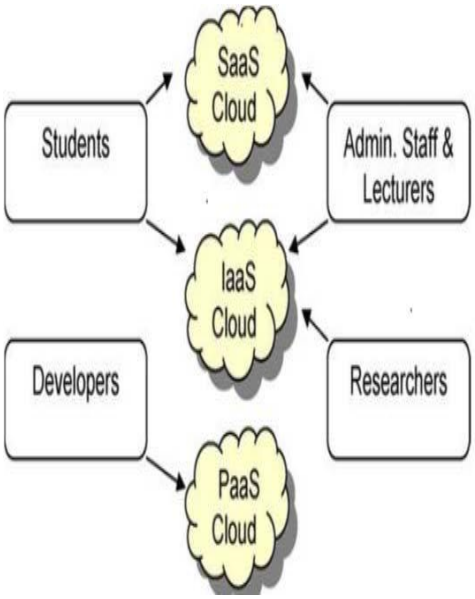

Fig 1. Cloud Services.

Cloud Computing, which can be associated to various kind of applications and Services that runs in wide spread network using basis resources and accessed by normal internet protocols and networking guidelines.

The main theme or scope of this proposed system it to assure the users by providing secure for the files stored in the cloud storage by providing a secret key for the file. The secret key is generated by advanced key management system. This is will be shared to the users. Our goal is to provide security and assure the users that files stored in the storage are encrypted and stored safety.

Related Work

Much of the data stored in clouds is highly sensitive, for example medical records and social networks. Security and privacy are, thus, very important issues in cloud computing.

User privacy is also required so that the cloud or other user do not know the identity of the user. Existing work on access control in cloud are centralized in nature. All other methods use ABE.

The scheme in asymmetric key approach and does not support authentication. It provides privacy preserving authenticated access control in cloud. However, the user take a centralized approach where a single key distribution centre (KDC) distributes secret key and attributes to all users.

Existing work on access control in cloud are centralized in nature. Except and, all other schemes use ABE. The scheme in uses a symmetric key approach and does not support authentication. The schemes do not support authentication as well. It provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Providing the security to data in clouds, they introduce a new privacy preserving authenticated access control. In existing environment, it stores information without knowing the user identity. Our environment supports the features of access control to decrypt the stored data only by a valid user, which will supports to construct, change and read the data storing in cloud. In this environment, a user can create a file and store it securely in the cloud.

This method consist the use of two protocols Attribute Based Encryption and Attribute Based Signature. The main advantage is to prevent replay attacks and supports construct, change, and understanding data stored in the cloud and Key distribution is done in a decentralized way. To protect the privacy of user attributes in the future. In token based computing, they often identify people by their attributes in the cloud. The security of the central authority and user privacy depends on the Performance of the attribute authorities. This work gives a more practice-oriented attribute based encryption system.

Disadvantages of Existing System:

- This method uses asymmetric key approach and also it does not support authentication.
- Cloud environment can be supported by very large number of users, so the existing system difficult to maintain large no. of users that are supported in a cloud environment.

Proposed System

We propose a new decentralized access control method for secure data storage in clouds that supports the anonymous authentication. KP-ABE and CP-ABE methods are studied for developing our new decentralized access control method. In the proposed method, the cloud verifies the authentication of the sequence without knowing the user's identity before storing data. Our method also has the added feature of access control in which only valid users are able to decrypt the stored information. This method prevents replay attacks and supports creation, modification and reading data stored in the cloud.

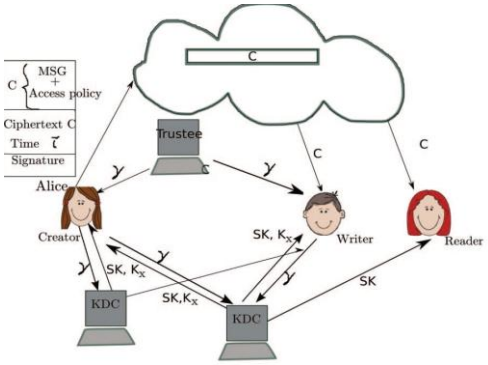

Fig 2: Proposed System.

We propose to use a decentralized access control technique to store data by providing security in clouds and also we hide the attributes and key access rule of a user. The cloud validates the authentication without knowing the users characteristics previous to the data store. By using this approach only authorized users have right to use the suitable attributes. By generating a secret key for each user independently, the security for the files stored in the cloud storage is increased.ABE can be viewed as an extension of the notion of identity-based encryption in which user identity is generalized to a set of descriptive attributes instead of a single string specifying the user identity. Compared with identity-based encryption , ABE has significant advantage as it achieves flexible one-to-many encryption instead of one-to-one; it is envisioned as a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control.There are two types of ABE depending on which of private keys or ciphertexts that access policies are associated with.

In a key-policy attribute-based encryption (KP-ABE) system, cipher texts are labeled by the sender with a set of descriptive attributes, while user's private key is issued by the trusted attribute authority captures an policy (also called the access structure) that specifies which type of cipher texts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast. For example, in a secure forensic analysis system, audit log entries could be annotated with attributes such as the name of the user, the date and time of the user action, and the type of data modified or accessed by the user action. While a forensic analyst charged with some investigation would be issued a private key that associated with a particular access structure. The private key would only open audit log records whose attributes satisfied the access policy associated with the private key. The first KP-ABE construction was provided by Goyal et al. , which was very expressive in that it allowed the access policies to be expressed by any monotonic formula over encrypted data. The system was proved selectively secure under the Bilinear Diffie-Hellman assumption. Later, Ostrovsky et al. proposed a KP-ABE scheme where private keys can represent any access formula over attributes, including nonmonotone ones, by integrating revocation schemes into the Goyal et al. KP-ABE scheme.In a ciphertext-policy attribute-based encryption (CP-ABE) system, when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the ciphertext, stating what kind of receivers will be able to decrypt the ciphertext. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority. Such a user can decrypt a ciphertext if his/her attributes satisfy the access policy associated with the ciphertext. Thus, CP-ABE mechanism is conceptually closer to traditional role-based access control method. The first CP-ABE scheme was proposed by Bethencourt et al. in, but its security was proved in the generic group model. Cheung and Newport [8] gave a CP-ABE construction under the Bilinear Diffie-Hellman assumption, but policies are restricted to a single AND gate. Later, Goyal et al. proposed a generic transformational approach to transform a KP-ABE scheme into a CP-ABE scheme using universal access tree. Their construction can support access structures which can be represented by a bounded size access tree with threshold gates as its nodes, and its security proof is based on the standard Decisional Bilinear Diffie-Hellman assumption. Unfortunately, in general this methodology would yield a ciphertext blowup of group elements for a Boolean formula of size , which limits its usefulness in practice. The most efficient CP-ABE schemes in terms of ciphertext size and expressivity were proposed by Waters in , the size of a ciphertext depending linearly on the number of attributes involved in the specific policy for that ciphertext. This is achieved by using advanced key management technique which provides the security for the files stored in the cloud storage by generating a secret key for each user. Key management technique which provides the security for the files stored in the cloud storage by generating a secret key for each user:Step 1: Choose two distinct prime numbers p an$q$.

Step 2: multiply $n = p*q$

Step 3: Compute $\varphi(n) = \varphi(p)\ \varphi(q)$, where φ Euler's totient function

Step 4: select an integer e $\varphi(n)$ are co-prime.(e is released as the public key exponent).Determine d as $d-1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative

inverse of *e* (modulo φ (*n*)).(This is more clearly stated as solve for *d* given $de \equiv 1 \pmod{\varphi(n)}$).
Encryption: c is a cipher text and m is a message
C=me (mod) n.
Decryption:

II. RESULT & ANALYSIS

The Home page of this implementation and result is as follows.

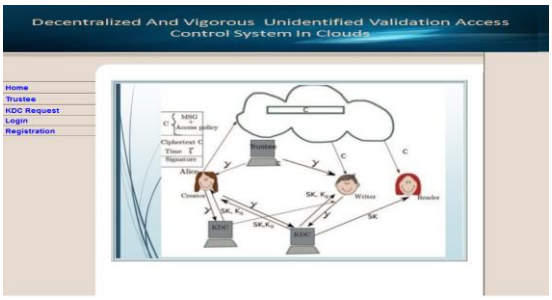

Fig 4:The Home Page.

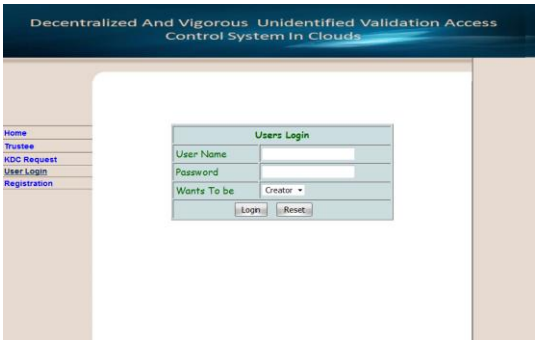

Fig 5: User Login: (creator, Writer, Reader).

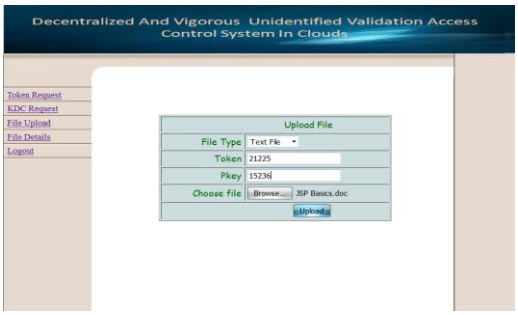

Fig 7:File Uploading.

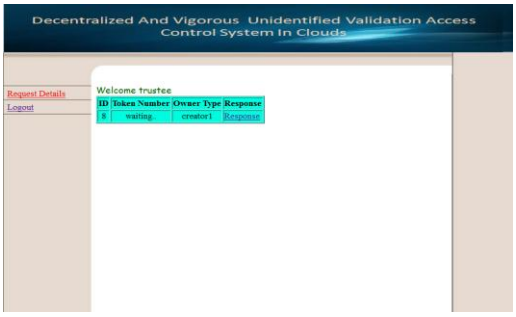

Fig 8:Requesting Details.

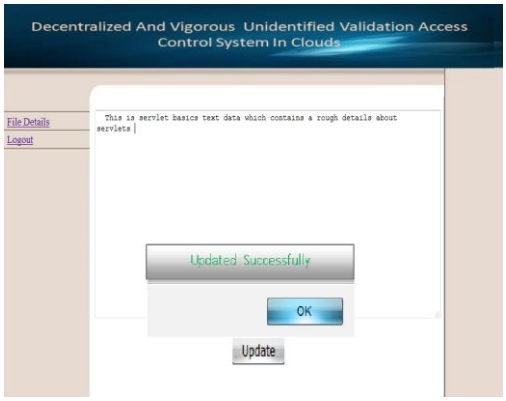

Fig 9: File and Password updating.

III. CONCLUSION

In this paper, we provide data security in a cloud storage using decentralized approach. We use a new decentralized access control technique to store data by providing security in clouds and also we hide the attributes and key permission rule of a user. The cloud validates the authentication without knowing the users characteristics previous to the data store. By using this approach only authorized users have right to use the suitable attributes. By generating a secret key for each user independently, the security for the files stored in the cloud storage is increased. This is achieved by using advanced key management technique which provides the security for the files stored in the cloud storage by generating a secret key for each user.

ACKNOWLEDGEMENT

Miss. Y.Hymavathi would like to thank Sri.CH.Samson, Assoc. Professor and B. Satyanarayana Reddy Assoc. Professor, HOD,Dept of CSE,who had been guiding throughout the project and supporting me. Also in giving technical ideas about the paper and motivating me to complete the work efficiently and successfully.

REFERENCES

[1] Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds Sushmita Ruj, Member, IEEE, Milos Stojmenovic, Member, IEEE, and Amiya Nayak, Senior Member, IEEE.
[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054. Springer, 2010, pp. 136–149.
[3] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," inCloudCom,ser.Lecture Notesin Computer Science, vol.5931. Springer, 2009, pp. 157–166.

[4] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.
[5] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," inTRUST,ser.Lecture Notes inComputer Science, vol.6101. Springer, 2010, pp. 417–429.
[6] G. Wroblewski, "General method of program code obfuscation," Ph.D. dissertation, Wroclaw University of Technology,2002,http://www.ouah.org/wobfuscation.pdf.
[7] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "Trustcloud: A framework for accountability and trust in cloud computing," HP Technical Report HPL-2011-38.
[8] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in 15th National Computer Security Conference, 1992.
[9] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to rolebased access control," IEEE Computer, vol. 43, no. 6, pp. 79–81, 2010.
[10] M. Li, S.Yu, K. Ren, and W.Lou, "Securing personal health records in cloud computing: Patient-centric andfine-grained dataaccesscontrol inmulti-owner settings," in SecureComm, 2010, pp. 89–106.