Secure of Data on stored Cloud from Decentralized Access Control with Anonymous Authentication

Vikas A V;
School of C&IT
REVA UNIVERSITY, Bengaluru, INDIA
vikasgowda.av@gmail.com

Prof. Nirmala S Guptha
Associate professor, dept of CSE
REVA UNIVERSITY, Bengaluru, INDIA
nirmalaguptha@revainstitution.org

***Abstract*— Decentralized storage system for accessing data with anonymous authentication provides more secure user authentication, control of Access is created on decentralized Key distribution center it is being more secure for data encryption. Generated decentralized Key which is from distribution center are taken and combined by key generation center. Our system provides which gives permission to user, in which only the particular system users are able to decrypt, view the stored information. User validations and access control scheme are introduced in decentralized this is useful for preventing replay attacks. The control of related access scheme is much more attract because it is very important to only few approval users have know to valid examine the result. Access control scheme prevents and supports creation replay attacks modifying and change in data stored in the cloud. The problems of validation, access control, privacy protection should be solved continuously.**

***Index Terms*—Key Generation Centre, Authentication,**
Attribute Based Encryption, Access Control.

I.INTRODUCTION

We already known that cloud is used to store data and the main issue in this is to protect data from unknown users rather than the authorized user's. Where data before entered in to cloud the data is encrypted using versus techniques by user.

In cloud computing some of the researchers are reached to their best mark obtaining a lot of attention from every area in world. Evolution, adoption of existing technologies and paradigms is cloud computing. This cloud computing is basically where users can outstate their computation and stores data/information to the cloud using the Internet. Most of data that can be stored in cloud like social networks, medical records which are highly sensitive and requires security. Privacy and security are thus very critical issues in cloud computing. Major thing is, the user should verify itself before initiating any transaction, and it must be protect that other users can not appropriateness of the user. There is need for other than technical solutions make sure that there safety, and privacy of the data. The cloud can hold the user for storage with for different purpose, and The cloud itself act for the services it provides.

II. LITERATURE SURVEY

Providing Security to data which is already stored in cloud is not easy as possible, the main issue is to protect data records from unauthorized users so we are implementing new ideas that are related to decentralized methodologies and must also check the anonymity of the user For example the user wants to post a comment on any recorded data but doesn't want his/her to any new information There are some of the cryptographic protocols methods such as Ring Signature, Mesh Signature Group Signature. The Ring Signature which means a more number of users has been involved so it is not feasible. The Mesh Signature which doesn't make any deference whether the message is from one user or from more number of users and which consists of information .The Group Signature it cannot be possible because of its already exist in the group For these kind of problem a new protocol ABS as been introduced in which the users have to be found or base something on associate with the data.

[1]Identity Based Authentication for Cloud Computing

In this identity based Cloud computing is one of the style of computing technique in which dynamically scalable and commonly virtualized resources are provided as a service over the Internet. This paper, first presents a novel Hierarchical Architecture for Cloud Computing. The Multi Identity-Based Encryption and Multi Identity-Based Signature for HACC is proposed. Finally an Authentication Protocol for Cloud Computing

[2] Distribution of access control in clouds using data

We are going to represent the new model for data store and identifying data in clouds. The concept of local accessing of data scheme of control which avoids storing repeated no of encrypted copies of same data, Cloud stores encrypted data (without being able to decrypt them). The main novelty of our

model is addition of key distribution centers. We propose Distributed Access Control in Clouds using data algorithm, where one or more Key distributed center keys to data owners and users. KDC may gives permission to access to particular fields of data in all records. Thus, a single key remove separate keys from owners file. Data Owner wants to encrypt the data along with the attributes it has and stores and get placed the cloud structure. The users with maximum same set of attributes can retrieved the data from the cloud structure. We apply attribute-based encryption based on bilinear pairings on elliptic curves. The scheme is collusion secure, two users cannot together decode any data that none of them has individual right to access. We show that our approach results in lower communication, computation and storage overheads, compared to existing models and schemes.

[3]Key-Policy Attribute Based Encryption using access control of data stored in cloud

Cloud computing is ongoing feature computing standard in which all types of assets the computing framework are given as a service through the Internet. As conforming as it may be the actual standard additional delivers a lot of people new challenge for providing security to data across the universe and access control when clients wants their protected data for offering on cloud servers, which are not inside the same trusted dominion as data possessors. The issue of at the same time supper grained scalability and data confidentiality of access control really still remains uncertain. The open source of key which as generated during encryption of message that characterizing and implementing access based policies on data quality and then moving towards the data owner to represent the majority of the calculation under takings included in fine-grained data access control to un-trusted cloud servers to the underlying data substance. We accomplish this goal by exploiting and combining techniques of decentralized key policy Attribute Based Encryption.

[4] Fuzzy Identity-Based Encryption

By taking of new concept to fuzzy based encryption scheme that we call Fuzzy Identity Encryption. In this approach many of the identified as sequence of easy attributes. A Fuzzy logical IBE scheme allows for a private key for an identity, ω, to decrypt a cipher text encrypted with an identity, ω 0, if and only if the identities ω and ω 0 are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be make over any to enable encryption using bio metric inputs as identity; The Fuzzy IBE scheme is precisely what allows for the use of biometric identifiers, which commonly have some sounds each time they are tested. We show that Fuzzy logical created IBE can be used for a type of application "attribute-based encryption". The fuzzy logic that helps in placing of data in queue which is in cloud. Basically Involvement of basic construction does not use any other database for search of files. We prove the security of our schemes under the Selective-ID security model.

[5] Towards Secure and Dependable Storage Services in cloud

A Cloud computing technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows customers and businesses prisons to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Perhaps the biggest concerns about cloud computing are security and privacy. There are many searching technique which were implemented in the cloud these technique supports only exact keyword search.

Cloud storage gives access permission to users for storing of their data and creation of the quality of data cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also replicable to user's possession of their outsourced data which avoid new security attacks towards the data by correcting of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, the selection of flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed erasure coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost by securing data this tells that more importance of data security dependable data storage on cloud computing.

[6] Cipher text-Policy Attribute-Based Encryption

By Previous encryption of recorded data in system concept which is used by the attributes to tells what exactly the encryption of applied data and also to provide some important policies into user's generated keys, from the system maintained by user's of attribute which is most commonly used data determines a policy for who can decrypt the data. In several distributed systems a user should only be able to access data if a user posses a certain set of crew denials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is

compromised, then the confidentiality of the data will be compromised. 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. Hence which is used as attributes to describe the encrypted of data and built policies into user's keys, Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control. In addition, we provide an implementation of our system and give performance measurements.

[7]Privacy Preserving Access Control with Authentication Securing Data in Clouds

A new privacy preserving authentication sachem of accessing control for providing of security to the data in clouds. By comparing to existing stored data in cloud we intend a new proposed scheme that cloud verifies and also identifies of the user without knowing the user's identity before storing information. The method of apply scheme also has the newly added a feature of control towards the certain data in which only valid normal users are able to decrypt the data which has been stored information. The scheme prevents some attacks and supports creation, change of data, altering and reading data stored in the cloud. Moreover, our authentication and access control scheme, unlike other access control designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

They presented a privacy access control scheme for clouds. This scheme not only provides supper-grained access control but also authenticate users who store their data in the cloud. Anyways the cloud cont identify the data of user that stored in cloud info structure, but only verifies the user's credentials. Key distribution is done in a decentralized way.

[8] Decentralized Access Control with Anonymous Authentication over Data Stored in Cloud

Generally knowing of new creation of decentralized authentication control for secured data store in clouds that supports anonymous authentication. In the proposed scheme the cloud looks and clarifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information Also address user revocation. The communication, computation, and storage overheads are comparable to centralized approaches,
Unknown who tries to attack the data they required the permission for entering into the cloud so only the concept of decentralizes has been used over the data.

[9] Multi-Authority Attribute Based Encryption

Multi Authority based encryption that user make to identify the searched the data whereas in attribute based encryption involves attribute to search the data. By introduced a single authority attribute encryption scheme and left the question whether the multiple authorities allowed distributing system. This scheme allows any poly number of independent authority to keep attributes and distribute secret keys.

In a multi identity based encryption scheme, each user is identified by a unique identity string. An authority attribute encryption scheme in contrast to scheme in which each user is identified by equal number of attributes, and some function of those attributes is used to determine decryption ability for each cipher text. Introduction of a single authority attribute encryption scheme and kept open the question of whether a scheme could be constructed in which multiple authorities were allowed to distribute attributes. An encryptor choose a file for each authorized users and a number of attributes he can make set.

III.EXISTING SYSTEM

1) Access control of information/data in the cloud is not decentralized in nature. All arranges that usages ABE or symmetric key strategy does not reinforce customer recognizing evidence. Earlier work gave insurance sparing affirmed access control in the cloud.

2) Work proposes Authority to renounce user traits with insignificant exertion. Cloud server is also responsible for suffering from information updating and server colluding attacks.

3) KDC is consolidated system where a lone KDC scatters secret keys and it attributes to all customers that are accessible. Single KDC is a solitary reason for disillusionment; with single riddle key frustration, a whole structure can fall.

4) There is no control of data in cloud before introducing decentralized technique, where anybody can access others files by just knowing the path which is linked to cloud.

IV.SYSTEM ARCHITECTURE

The model explains that, there are three users 1.creator 2.writer 3.reader, where creator receives a request message from trustee that provide an permission to grant to write a data by giving an secrete key after once a key is generated by admin any time file can to written from cloud, hear there

will be a common key for reader and writer which is KDC,

In this a file before entering into cloud which is encrypted by admin or creator along with the signature once it has encrypted that trusted party can decrypt that message by asking permission for group creator and can get original data

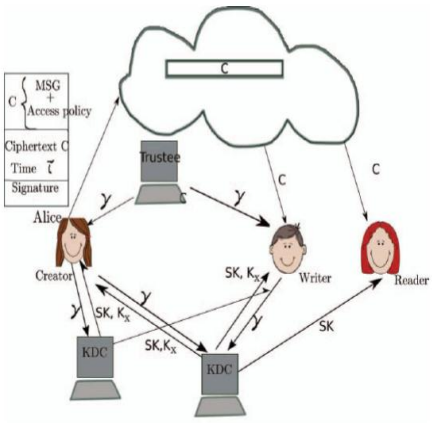

Fig1: secure data on cloud storage model

V.FLOW CHART

A flow chart is one of the type of diagram which explain about the representation of algorithm and process sequence which gives a solution for a particular problem process operation represents boxes, arrows, that represents flow of control, flow chart is used to analyze, designee in various fields

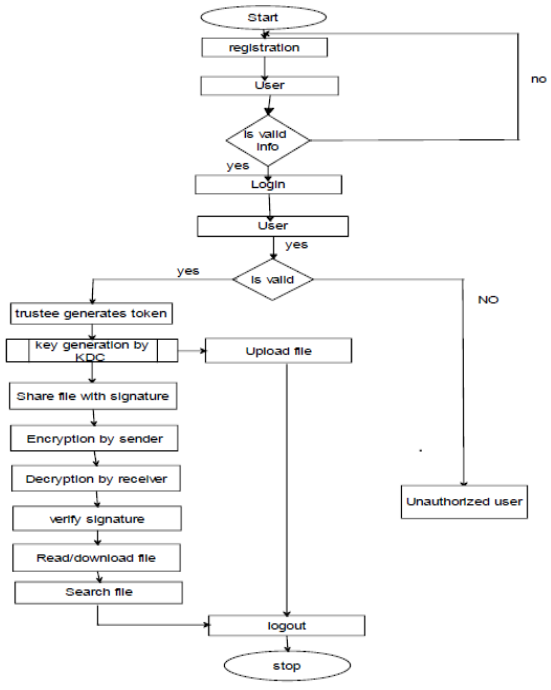

Fig2: flow chart

VI.PROPOSED MODEL

The proposed decentralized approach does not authenticate while accessing the cloud by user he/her wants to remain same as new user. And uses attribute based signature scheme to achieve authenticity and privacy. Decentralized scheme has the added feature of control accessing in only which is valid users who can be able to protect and decrypt there data information. It prevents replay attacks and supports creation, modification, and reading data stored in the cloud.

1. Based upon on user information the security is provided to Access control their policies for user will be assigned and with the access policies anonymous authentication is given to the user who wants to store secure data on cloud.

2. By generation of secret key access permission is granted on authorized users.

3. Providing security to data on the basis access policy control technique. Security controls are always to be safe guards or different measures to avoid counteract or minimize security level of risks relating to personal property.

V. CONCLUSION

Decentralized framework gives secure information stockpiling on cloud with the unknown verification. Decoding of document is permitted just for framework approved/confirmed clients. This approach that supports to avoid and prevention of some attack, creation, modification, viewing the information that stored in the Cloud. The information which can be access in cloud can be verified by authorized user's in distributed decentralized combined network and which is very useful and strong there for overall communication storage has been developed by comparing to the centralized and decentralized methods.

REFERENCES

[1] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," *Proc. First International Conference. CloudComputing*, 2012.
[2] SS. Ruj, Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," *in IEEE TrustCom, 2011.I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism*, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963,
[3]S.Seenu Iropia and R.Vijayalakshmi (2014), "Decentralized AccessControl of Data Stored in Cloud using Key-Policy Attribute Based Encryption" in preceedings
[4]A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," *Pro.Anual. International conference.in Advances in Cryptology*, 2005.
[5] C. Wang, and W. Lou, Toward Secure and Dependable Storage Services in Cloud Computing, Apr.- June 2012.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute- Based Encryption," 2015.
[7] SS. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", International Symposium on Cluster, Cloud and Grid Computing, 2012.
[8] S Sushmita Ruj, Milos Stojmenovic and Amiya Nayak, Decentralized Access Control with Anonymous Authentica-tion of Data Stored in Clouds_ , *IEEE Transactions on Parallel and Distributed* 220
[9] M. Chase, "Multi-Authority Attribute Based Encryption,", 2014.
[10] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in CloudComputing",2012.