RESEARCH ARTICLE OPEN ACCESS

Secure Cloud Storage using Access Control with Anonymous Authentication

Dr. Sreepathi B [1], Santhamma [2], Anjana Naidu A [3], Archana l [4]
Chinta Praveena Lakshmi [5], Preethi J [6]
Head of the Department [1]
Department of Information Science and Engineering
VTU/RYMEC, Ballari
Karnataka - India

ABSTRACT
We propose a new 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. Our 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. We also address 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, computation, and storage overheads are comparable to centralized approaches.
Keywords :- Anonymous, Authentication, Decentralized, Centralized

I. INTRODUCTION

Cloud computing is a promising computing model which currently has drawn far reaching consideration from both the educational community and industry. By joining a set of existing and new procedures from research areas, for example, Service-Oriented Architectures (SOA) and virtualization, cloud computing is viewed all things considered a computing model in which assets in the computing infrastructure are given as services over the Internet. It is a new business solution for remote reinforcement outsourcing, as it offers a reflection of interminable storage space for customers to have data reinforcements in a pay-as- you- go way.

It helps associations and government offices fundamentally decrease their financial overhead of data administration, since they can now store their data reinforcements remotely to third- party cloud storage suppliers as opposed to keep up data centres on their own. Numerous services like email, Net banking and so forth… are given on the Internet such that customers can utilize them from anyplace at any time. Indeed cloud storage is more adaptable, how the security and protection are accessible for the outsourced data turns into a genuine concern. The three points of this issue are availability, confidentiality and integrity.

To accomplish secure data transaction in cloud, suitable cryptography method is utilized. The data possessor must encrypt the record and then store the record to the cloud. Assuming that a third person downloads the record, they may see the record if they had the key which is utilized to decrypt the encrypted record. Once in a while this may be failure because of the technology improvement and the programmers. To overcome the issue there is lot of procedures and techniques to make secure transaction and storage.

User Privacy in Cloud Computing

User privacy is also required in cloud. By using privacy the cloud or other users do not know the identity of the other user. The cloud can hold the user accounts for the data in cloud, and likewise, to provide services the cloud itself is accountable. The validity of the user who stores the data is also verified. There is also a need for law enforcement apart from the technical solutions to ensure security and privacy.

The cloud is also prone to data modification and server colluding attacks. The adversary can compromise storage servers in server colluding attack, so that server can modify data files even though the servers are internally consistent. The data needs to be encrypted to provide secure data storage. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

Search on Encrypted Cloud Data

Efficient search on encrypted data is also an important fear in clouds. The clouds should not know the query but it can able to return the records that satisfy the query. Searchable encryption used to achieve this scheme.

Security and privacy protection on cloud data

Users Authentication scheme using public key cryptographic techniques in cloud computing. Many homomorphic encryption techniques have been optional to ensure that the cloud is not able to read the data while performing computations on the data. By using this encryption scheme, the cloud receives cipher text of the data and performs computations on the cipher text and returns the encoded value of the result to user then the user is able to decode the result, even though the cloud does not know what data it has operated on. In such circumstances, it must be probable for the

II. LITERATURE SURVEY

1) "Privacy Preserving Access Control with Authentication for Securing Data in Clouds,"
AUTHORS: S. Ruj, M. Stojmenovic, and A. Nayak
In this paper, we propose a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information. Our 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. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

2. **"Toward Secure and Dependable Storage Services in Cloud Computing"**
AUTHORS: C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou
Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

3. **"Cryptographic Cloud Storage,"**
AUTHORS: S. Kamara and K. Lauter,
We consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. We describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal. We survey the benefits such an architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

4. **"Identity-Based Authentication for Cloud Computing,"**
AUTHORS: H. Li, Y. Dai, L. Tian, and H. Yang
Cloud computing is a recently developed new technology for complex systems with massive-scale services sharing among numerous users. Therefore, authentication of both

users and services is a significant issue for the trust and security of the cloud computing. SSL Authentication Protocol (SAP), once applied in cloud computing, will become so complicated that users will undergo a heavily loaded point both in computation and communication. This paper, based on the identity-based hierarchical model for cloud computing (IBHMCC) and its corresponding encryption and signature schemes, presented a new identity-based authentication protocol for cloud computing and services. Through simulation testing, it is shown that the authentication protocol is more lightweight and efficient than SAP, specially the more lightweight user side. Such merit of our model with great scalability is very suited to the massive-scale cloud.

5.**"Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,"**

AUTHORS: M. Chase and S.S.M. Chow

Attribute based encryption (ABE) [13] determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase [5] gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every ciphertext, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which unnecessarily compromises the privacy of the user. In this paper, we propose a solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice.

III. EXISTING SYSTEM

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.

DISADVANTAGES OF EXISTING SYSTEM:

- The scheme in uses asymmetric key approach and does not support authentication.
- Difficult to maintain because of the large number of users that are supported in a cloud environment.

IV. PROPOSED SYSTEM

We propose a new 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.
- Our 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.

ADVANTAGES OF PROPOSED SYSTEM

- Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them.
- Authentication of users who store and modify their data on the cloud.
- The identity of the user is protected from the cloud during authentication.

V. MODULES

- System Initialization Module.
- KDC Module
- Trustee Module
- Signature Module.

MODULES DESCRIPTION:

System Initialization:

- We present our cloud storage model, adversary model and the assumptions we have made in the paper.
- The cloud is honest-but-curious, which means

- that the cloud administrators can be interested in viewing user's content, but cannot modify it.
- Users can have either read or write or both accesses to a file stored in the cloud.
- All communication between users/clouds are secured.
- To write to an already existing file, the user must send its message with the claim policy as done during file creation. The cloud verifies the claim policy, and only if the user is authentic, is allowed to write on the file.
- **KDC Module:**

- We emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. The architecture is decentralized, meaning that there can be several KDCs for key management.
- Attribute generation.
- The token verification algorithm verifies the signature contained in γ using the signature verification key TV er in TPK.

- **Trustee Module:**
- A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token.
- There are multiple KDCs, which can be scattered. For example, these can be servers in different parts of the world.
- A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing.

- **Signature Module:**
- The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim.
- The ciphertext C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message.
- The verification process to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs

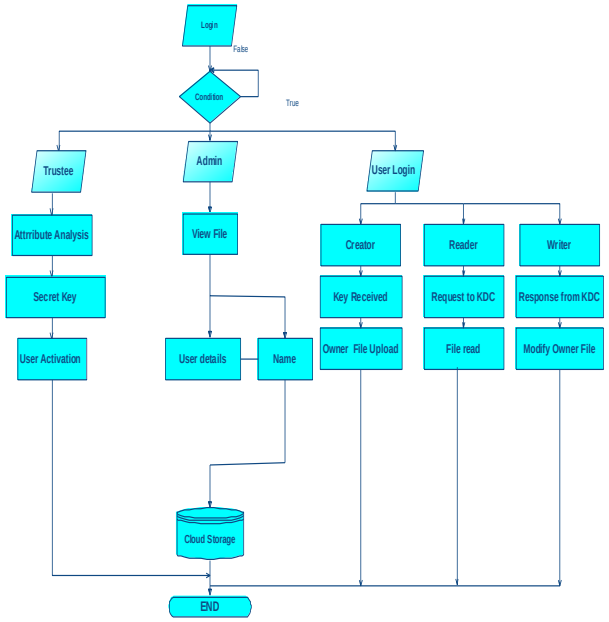
Table 1:-Comparative Study on Existing vs. Proposed System

SN	TECHNIQUE	EXISTING	PROPO
1	**Approach**	Centralized	Decentrali
2	**Key Encryption**	Use ABE(Attribute Based E	Use KDC(Key Distributi on
3	**Authenticatio n**	Does Not Provide Authentication	authenticat e the validity of the message without
4	**Type Of Key**	symmetric key	Public
	Attack Model	Resistant to replay attacks,	Resistant to

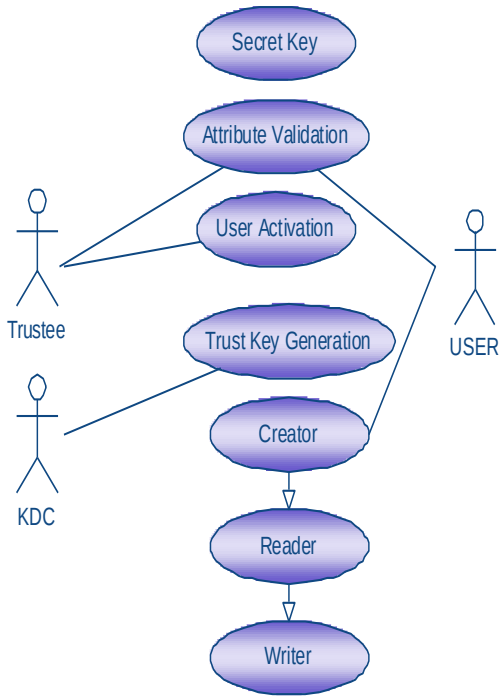
VI. DATA FLOW DIAGRAM

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of

abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



Use case diagram.



VII. CONCLUSION

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.

ACKNOWLEDGMENT

We would like to thank my guides and parents who helped us in preparing this paper.

REFERENCES

[1] Sahai and B. Waters, "Fuzzy Identity- Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

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

[3] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion- Resistance," IACR Cryptology ePrint Archive, 2008.