A NOVEL DECENTRALISED SCHEME FOR IDENTITY PRESERVED ACCESS CONTROL IN CLOUD

Assistant Professor (Sr), VIT University, Vellore, Tamil Nadu, India.
UG Scholar, VIT University, Vellore, Tamil Nadu, India.
UG Scholar, VIT University, Vellore, Tamil Nadu, India.
Email: pgshynu@vit.ac.in

Abstract:
Cloud computing has become a recent trend in the software industry due to its advantages like flexibility, efficiency, manageability and many others. Though many advantages are there in the cloud, it has its own security concerns. In the proposed scheme the following security concerns in the cloud are to be addressed access control, data privacy and also identity privacy. Most of the research work concentrates mainly on data confidentiality and access control whereas less attention is paid to identity privacy. So hereby we propose a decentralised scheme with fine-grained access control to the data stored in the cloud. Data confidentiality is achieved with CP-Attribute Based Encryption Scheme and for Identity Privacy and Access Control a decentralised scheme has been proposed which ensures higher rates of security and user identity privacy.

Keywords: Cloud Computing, Access Control, Identity Preservation, Data Confidentiality.

I. Introduction
Cloud computing is one of the most valuable innovations for business, providing cheap virtual services that once required expensive local hardware. We will be able to place almost everything in the cloud. The cloud is only going to become more important to us, and we must find ways to protect our data while getting the high-quality performance we need. A large part of performance means adequate security is a must.
Cloud Computing have several security challenges like Data Breaches, Data loss and leakage, Service traffic hijacking, Insecure interfaces and API, Denial of Service and Distributed Denial of Service attacks, Malicious users and insiders, user identity privacy etc. Here in the proposed scheme, three main issues are to be addressed Data Confidentiality, the Access control and User Identity Privacy.
Restriction of users to the information stored in the cloud is very much important. Only authorised users should be allowed to access the data stored in the cloud, and it is the need for access control in the cloud. When sensitive computation tasks are outsourced, they are beyond the user control. So therefore not only the users but also the operations performed on data must be controlled. Moreover, this is known as data confidentiality. The users identity must also be protected as based on the identity of the user only authentication techniques are controlled and moreover now a days the users are more concerned about their identity in the public domains so user identity preservation is also important. Most of the research work concentrates mainly on data confidentiality and access control whereas less attention is paid to identity privacy. So at this moment in this project concentration is more on user identity privacy by decentralising the central authority and thus limiting the identity leakage.

II. Related Work

In [1] the author has discussed problems associated with access control, authentication and privacy protection have been addressed. A decentralised access control scheme has been used. (i.e.) key distribution is not dependent on one single KDC. Any number of KDC can be used for Key distribution. Attribute Based Access Control Scheme is used here. Moreover, an unauthorised user cannot encrypt or decrypt the data, and this is also collusion resistant. Authentication is ensured by allowing only the valid users registered to receive the key and the attributes from the KDC. User’s privacy is preserved by allowing only the users with accurate attributes to access the data and also those attributes and user information can be viewed only by cloud trustees. In [2] the author has proposed the design of a secure RBAC based cloud storage system where the access control policies are enforced by role-based encryption (RBE). This RBE scheme enforces RBAC policies on encrypted data stored in the cloud with an efficient user revocation. In RBE scheme, the owner of the data encrypts the data in such a way that only the users with appropriate roles as specified by an RBAC policy can decrypt and view the data. In [3] the author has proposed a scheme of control data access in cloud computing based on the trust that is evaluated by the data owner and the reputations that are generated by a number of reputational users by applying Attribute-Based Encryption and Proxy Re-Encryption. Here the concept of context-aware trust and reputation evaluation of the data owners and consumers in a cryptographic situation is proposed here. In [4] the author has proposed a scheme where it is possible for the server only to know some of the users acquired attributes, yet it does not know the complete identity of the user. Also, a k-times limit for anonymous access control is provided. That is, it is possible for the server to limit a particular set of users (i.e., those users with the same set of attribute) to access the system for a maximum of k-times within a period.
or an event. Thus role based access control along with identity privacy is achieved here in this paper. In [5] the author has proposed a trust model of role-based access control. Role inheritance, Role hierarchy and role trust-worthiness are also discussed here in this paper. The data owners will be evaluating the trust on the roles in an RBAC system, and they will use this trust evaluation to decide whether to store their encrypted data in the cloud for a particular role. These trust models can be used to control and remove users who have bad historical behaviour and thus the malicious users can also be identified. In [6] the author has discussed the following concerns in cloud computing access control, data privacy and also identity privacy. The author has clearly stated that not only data confidentiality but also identity privacy is also a must. So to protect the user identity, two main algorithms were proposed, one with fully anonymity protection algorithm and other with semi-anonymity protection algorithm. In [7] the author has proposed a Cipher Text Policy-Attribute Based encryption for cloud storage systems. Moreover, also have made the system decentralised with multiple Attribute Authorities instead of a single and central attribute authority, and hence the identity leakage could be minimised. The author has also adopted Pederson commitment scheme along with Oblivious Commitment-Based Envelope for cryptographic key distribution. The users of the cloud receive the keys based on their identified attributes, and the Attribute authorities will not be able to pool the user identities with the help of user provided attributes. In [8] the author proposes a decentralised access control scheme with user revocation. For a decentralised access control, the author uses the LSSS access structure. Moreover, the multi-authority Attribute Based Encryption overhead is avoided with the help of a Proxy server. All the computational overhead is passed on to the proxy server. In [9] the author proposes an Intelligent Role Based Access control technique. The model mainly consists of two components the temporal extensions and the intelligent agents. The user is divided into normal users and malicious users. If identified as malicious users they are subjected to intelligent temporal level clarification systems. Their temporal constraints and user activity history are all studied before they are allowed to access the cloud and this is the duty of the security manager component of the cloud. The author proposes a trust and reputation based access control in [10]. The trust and reputation are evaluated by the data owner and the reputation centres with the help of Attribute based encryption and Proxy Re-Encryption techniques. And this paper also proposes a reputation based user revocation scheme for further more security.

III. System Design and Implementation

As discussed, the main objective of our system is to provide access control, data confidentiality and identity privacy. The consumers and owners of the data in the cloud are to be approved by the central authorities known as attribute
authorities. Instead of handling the authority to a single person, the authority is divided between numbers of persons thus limiting the identity leakage. Thus user identities are preserved with the help of a decentralised admin. Data confidentiality is achieved with the help of attribute-based encryption and to ensure more access control One Time Password comes into the scenario.

A. Architecture specification

Our goal is to achieve a multi-authority CP-ABE which thereby achieves the required security as defined above; this guarantees the confidentiality of the cloud user identity information provided by them at the time of registration; and also tolerates compromise attacks on the cloud authorities or the collusion attacks due to cloud authorities.

![System Model of Our Scheme](image)

**Fig 1: System Model of Our Scheme.**

**N- Attribute Authorities:** It is the responsibility of the attribute authority to accept and reject the requests. This is done based on the Privilege tree scheme. The following privileges are allowed on the data uploaded in the cloud. Read mine, Read all, Delete, Modify, Create. Every operation is associated with one of the privilege p specified above, which is described by a privilege tree T_p. If the user attributes satisfy a node in a privilege tree, then only the user is allowed to access the data stored in his allowed privilege. Thus fine-grained access control is achieved which is suitable for the cloud storage device.

**Cloud Server:** The Cloud Server is said to have the required storage capacity, and its main job is to store them. The cloud server can execute an operation of privilege p if and only if the user’s credentials are verified through the privilege tree T_p.

**Data Owners:** The Owners should register with cloud server to upload file and data with their allotted size and within the period of time.

**Data Consumers:** The Data Consumers should register with the cloud server and get the permission from N-Attribute Authority to log in. Then select the files from the cloud server and give request to N-Attribute Authority get file key for download process.
B. Proposed Method

The main contributions of this paper are the following:

1) This allows Distributed access control of data stored in the cloud so that only authorised users and also with only valid attributes can only access them.

2) This provides Authentication of users who store and modify their data on the cloud.

3) The user identity is protected from the cloud during the time of authentication.

4) The access control and the authentication done are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually unauthorised.

5) This proposed protocol supports multiple reads and writes to the data stored in the cloud.

We now hereby assume that the cloud servers are semi-honest and are also assumed to behave most of the time properly, but the collusion of malicious data owners and consumers may often happen to gain illegal profits. But when the protocol is correctly followed, and the requests are processed correctly then legal benefits are said to be gained.

C. Security Model

Let us consider N attribute authorities are to be untrusted. And even though if they follow the protocol generally these attribute authorities are interested in the user activities and try to find out as much information as possible individually. However, we can relax the above assumption, and the collusion could be allowed between the authorities. Data Consumers are untrusted since they could collude with genuine users and could illegally access what they are not allowed to. Besides we need not consider the identity leakage because this can be prevented by employing network protocols. To formally define the security of our cloud scheme, we first give the following definitions.

Fig 2: System Architecture.
Setup: This algorithm takes inputs such as the systems security parameters. Attributes authorities are only allowed to execute this algorithm to jointly compute a system-wide public parameter.

Key Generate: This algorithm enables a user to interact with every attribute authority, and obtains a private key corresponding to the input attribute set.

Encrypt: This algorithm takes as input the public key, a message M, and a set of privilege trees, where r is determined by the encrypter. It will encrypt the message M and returns a cipher text and a verification set so that a user can execute a specific operation on the cipher text if and only if his attributes satisfy the corresponding privilege tree.

Decrypt: This algorithm will be used at file controlling (e.g. reading, modification, and deletion). It takes as input the public key, a cipher text, and a private key, which has a set of attributes and corresponds to its holder’s. If the set satisfies any tree in the set, the algorithm returns a message or a verification parameter. If the verification parameter is successfully verified by Cloud Servers, who use to verify it, the operation request will be processed. For a cloud user to register into the system, the user must provide the necessary details asked by the authorities at the time of registration.

The attribute authority is not centralised in a single entity. There should be in odd numbers. Thus the maximum number of authorities’ approval will be taken into account. When to the registered user is authenticated and have given their clearance the user is now authenticated to log in and receive the secret keys and their one-time passwords to their registered attributes. A data owner or a data consumer can login into the system by presenting her details given during the time of registration.

The attribute authority now provides the data or consumer with a secret key. The files are encrypted with the access policy. To prove the authenticity of the logging in consumer or owner they should enter the key provided by the attribute authority and the authenticity of the key will be checked. Then only the cloud user will be allowed to log in and do their required operations on the cloud. If a consumer wants to download a file, the request for the file’s secret key is sent to the attribute authority.

Then the attribute authority sends the secret key to the registered attributes of the user such as email or phone number. And now if the correct secret key is issued the user can download the file. Thus a completely secured system is proposed and a multi-authority scheme that achieves security and tolerates the compromise attacks on the authorities and the collusion attacks by the authorities is proposed.
IV. Conclusion

Thus a decentralised cloud access scheme which addressed the three main issues of cloud security access control, data confidentiality and identity privacy is proposed and implemented. Access Control is implemented with providing one-time passwords and validating the users before they are enrolled to cloud the identity leakage is minimised by decentralising the user attributes between authorities and data confidentiality with a secure encryption scheme. More efficient methods of user revocation and key distribution could be added to this cloud scheme to make this more effective in future.

References


**Corresponding Author:**

**Shynu P. G***,

**Email:** pgshynu@vit.ac.in