International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Survey on Access Control Scheme for Data in Cloud with Anonymous Authentication

Manju Lakshmi[1], Anju Rachel Oommen[2], Smita C Thomas[3]

[1, 2, 3] Mount Zion College of Engineering, Kadamannitta, Pathanamthitta, Kerala

Abstract: ***Cloud data is a generation technology, it is efficiently support the client oriented service. Cloud computing is a computing concepts. It enables when required and low maintenance usage of resources. The data to some cloud servers and various privacy related concerns emerge from it. Access Control methods ensure that authorized users access the data and the system. This paper discusses various access control scheme used in the cloud data.***

Keywords: Access control mechanism, Authentication, attribute-based encryption, cloud Computing

1. Introduction

Cloud computing has been considered as a new model of enterprise IT infrastructure, which can organize huge resource of computing, storage and applications, and enable users to enjoy ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources with great efficiency and minimal economic overhead In a multiauthority 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 [3] gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group. As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group. Cloud computing is revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a cloud. Cloud computing system should be salient in the case of security in which some part of the system is compromised by attackers. Anony Control to address to the data privacy, and the user identity privacy in existing access control schemes. The data access privilege will be depending upon misbehaviour of user in cloud server. Cloud is used in many applications like in medical and social networks were the data stored in cloud is highly sensitive. The important key factor is security and Privacy. The most important concern in cloud is encrypted data. The cloud must return the records and satisfy the query, regards unknowing the exact query which can be achieved by searchable encryption.

Access control is generally a policy that allows, or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control is also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security. Various access control models are there that is Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these models are basically known as identity based access control models. In all these access control models, user (subjects) and resources (objects) are identified by unique names. Identification may be done directly assigned to the subjects. These access control methods are effective in unchangeable distributed system. There are only a set of Users with a known set of services. Nowadays, very large distributed open systems are developing very rapidly. These include Grid Computing and Cloud Computing. These systems are like virtual organizations with various autonomous domains. The relationship between users and resources is dynamic and more ad-hoc in cloud and inter cloud systems. In these systems, users and resource providers are not in the same security domain. Users are normally identified by their attributes or characteristics and not by predefined identities. In such cases, the traditional identity based access control models are not very much effective and therefore, access to the system must be done on decisions based on certain attributes.

The Attribute-Based Signatures (ABS), a flexible primitive that permits a gathering to sign a message with fine-grained control over recognizing data. In ABS, an sponsor, who has an arrangement of characteristics from the power, can sign a message with a predicate that is fulfilled by his characteristics. The mark uncovers close to the way that a solitary client with some arrangement of traits fulfilling the predicate has confirmed the message. Specifically, the mark shrouds the credits used to fulfil the predicate and any distinguishing data about the underwriter (that could interface numerous marks as being from the same endorser). Moreover, clients can't conspire to pool their qualities together.

2. Literature Survey

Cloud computing [1] permits the original of information outsourcing. Therefore to shieldinformation privacy, delicate information must be encrypted before they're outsourced to the financial cloud that creates the effective information utilization service a difficult task. Albeit searchable cryptography technique permits users to firmly search over encrypted information through keywords, they support solely Boolean search. They're not however decent to satisfy {the information the info the information} utilization effectively as a result of theirs innately demanded by sizable amount of

users and data files placed in cloud. Therefore it's necessary to permit multiple keywords within the search request and come back documents within the order of their connation to the keywords. The Boolean keyword search technique solely produces the unsorted result. An efficient methodology projected for this difficult drawback is privacy protective search over encrypted cloud information. This methodology establishes a group of privacy necessities for secure cloud information utilization system through cacophonic the cloud information and storing the chunk information in several servers when the information has been encrypted and outsourced by the information owner. Among totally different multi-keyword sociology, this methodology chooses the economical similarity live of "coordinate matching" for looking technique. Then in line with prime K question methodology the sorted results area unit created.

Much of the information [2] keep in clouds is extremely sensitive, for instance, medical records and social networks. Security and privacy are, thus, vital problems in cloud computing. In one hand, the user ought to manifest itself before initiating any group action, and on the opposite hand, it should be ensured that the cloud doesn't tamper with the information that's outsourced. User privacy is additionally needed so the cloud or different users don't apprehend the identity of the user. We propose a replacement decentralized access management theme for secure information storage in clouds that supports anonymous authentication. Within the planned theme, the cloud verifies the believability of the series while not knowing theuser's identity before storing information. Our theme additionally has the further feature of access management within which solely valid users are able to decode the keep info. The theme prevents replay attacks and supports creation, modification, and reading information keep within the cloud. We have a tendency to additionally address user revocation. Moreover, our authentication and access management theme is decentralized and strong, not like different access management schemes designed for clouds that are centralized. The communication, computation, and storage overheads are equivalent to centralized approaches.

In this paper [3] Information access control is a viable approach to guarantee the information security in the cloud. Then again, because of information outsourcing also, untrusted cloud servers, the information access control gets to be a testing issue in distributed storage frameworks. Existing access control plans are no more appropriate to distributed storage frameworks, since they either create different scrambled duplicates of the same information or require a completely trusted cloud server. Cipher text-Policy Trait based Encryption (CP-ABE) is a promising strategy for access control of scrambled information. It requires a trusted power deals with every one of the traits and circulates keys in the framework. In distributed storage frameworks, there are variouspowers exist together and every power can issue qualities' freely. Nonetheless, existing CP-ABE plans can't be specifically connected to the entrance control for multi-power distributed storage frameworks, because of the wastefulness of unscrambling and renouncement. In this paper, we propose DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), a viable and secure information access control plan with effective decoding and disavowal. In particular, we build another multi-power CP-ABE plan with proficient unscrambling furthermore plan an effective characteristic renouncement strategy that can accomplish both forward security and in reverse security. The investigation and the recreation results appear that our DAC-MACS is exceedingly effective and provably secure under the security model.

In this paper [4] the Property based encryption (ABE) is another vision for open key encryption that permits clients to encode and decode messages in light of client qualities. For instance, a client can make a cipher text that can be decoded just by different clients with properties fulfilling ("Faculty" OR ("PhD Student" AND "Quals Completed")). Given its expressiveness, ABE is at present being considered for numerous distributed storage and registering applications. On the other hand, one of the fundamental effectiveness disadvantages of ABE is that the span of the cipher text and the time required to unscramble it develops with the many-sided quality of the entrance recipe. In this work, we propose another worldview for ABE that to a great extent wipes out this overhead for clients. Assume that ABE cipher texts are put away in the cloud. We demonstrate how a client can furnish the cloud with a solitary change key that permits the cloud to interpret any ABE cipher text fulfilled by that client's characteristics into a (consistent size) El Gamal-style cipher text, without the cloud having the capacity to perused any piece of the client's messages. To correctly characterize and show the upsides of this methodology, we give new security definitions to both CPA and replay able CCA security with outsourcing, a few new developments, a usage of our calculations and point by point execution estimations. In a ordinary arrangement, the client spares altogether on both transmission capacity and unscrambling time, without expanding the number of transmissions.

3. Architecture View

Cloud computing is a delivered computer services over the network. Cloud computer kind of computing where by resources and it related capabilities are provided as services to the outer customer using Internet technique. Cloud computer environment for providing information resources that are delivered as services to the end user over the internet on demand cloud is defined with file essential characteristics.

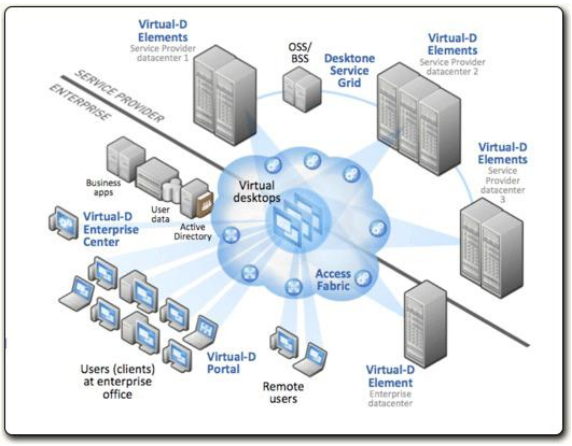

Figure 1: Could computing environment

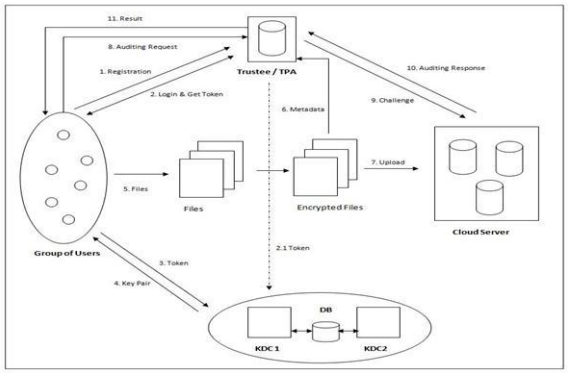

Figure 2: System Architecture

4. Conclusion

The decentralized access control technique with anonymous authentication, which prevents replay attacks and stores data securely at cloud server. The cloud does not know the identity of the user who stores information, but only verifies the user as credentials. Key distribution is done in a decentralized way. Third Party Auditor is used to reduce the burden of user from auditing or Integrity checking techniques which don't know about the keys and original data or encrypted data uploaded by user at cloud server. Third Party Auditor also performs the task of Batch Auditing. One limitation of the cloud knows the access policy for each record stored in the cloud. In Future, More attributes can be selected to provide more complex access structure. In this system if new file with same filename is uploaded old file gets overwrite so we can check the Duplication of data before storing the new copy.

5. Acknowledgement

We would like to thank, first and foremost, Almighty God, without his support this work would not have been possible. We would also like to thank all the faculty members of Mount zion college of engineering, for their immense support.

References

[1] S Preethi, V Shanmugavalli, H Kezia "Privacy Conserving in Cloud Documents Over Cloud Server with Efficient mrse
[2] Hemalata, V. Balaji, P. Nirupam, "Anonymous Authentication for Decentralized Access Control of Cloud data.
[3] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc.IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556- 563.
[4] R. Vishnu Sekhar, N. Nandini, D. Bhanumathy, M. Hemalatha "Identity Based Authentication for Data Stored in Cloud