Access Control in Cloud Computing Based on KP-ABE Encryption on Certificates

Amrata Shrivastava
M.Tech Scholar, Department of CSE
SIRT Bhopal, INDIA
E-mail- amratashrivastava@gmail.com

Dr. Rajiv Shrivastava
Professor, Department of CSE
SIRT Bhopal India
E-mail- drrajiv_sri@yahoo.co.in

ABSTRACT
It is quite difficult to keep up all necessary data in secure manner where it has the necessity for various usages for users in cloud. Cloud service is centered on Web Service area, and it will face all types of security issues comprising what Web Services aspect. Security is the main concern for development of the cloud services. In this paper we discuss access control in cloud computing for security aspect. In this paper we proposed a model which provide the security through attributes (certificates and policies) by KP-ABE (Key Policy Attribute based Encryption); KP-ABE is an advance public key cryptography primitive for one-to-many connections**.**

Keywords—Access Control; Data security; Data availability; Cloud computing.

INTRODUCTION
The usage of web and novel technologies today, for commerce and for these clients, is even now a part of living. Any data is accessible at anyplace within the world at any time. Few years ago that wasn't probable [1]. Today it have risen lots of prospects of right to use to public and personal data like web speed access or the readying of mobile dispositive that enable the joining to web from virtually all over. Nowadays lots of individual's are accessing their mail on-line through webmail shoppers, writing cooperative documents victimization net browsers, making computer-generated albums to transfer their pictures of the vacations. They're active apps and storage data in servers situated in web and not in their own terminals. Something as straightforward as enter in an exceedingly web content is that the solely thing a user must begin to usage the services that exist in on a far off server and lets him share non-public and personal info, or expending computing cycles of a mound of servers that he can ever see with his own eyes [2]. And each day its getting used a lot of these facilities that are known as cloud workstation service area. That term is given as a result of the trope regarding web, as one thing than the client see sort of a cloud and can't see what's within.

Cloud computing is a global source where user wish to keep all his data with safety dimension, through this many application, program and computational concepts can grow complete profits via this technology without any confined physical storage device and server for his data storing. These facilities and services are generally distributed into three classes as:-

- Infrastructure-as-a-Service.
- Platform-as-a-Service and
- Software-as-a-Service [3] [4].

Access control is one of the utmost significant security system in cloud service, and Cloud service can not applicable on old access control model to attain access control due to its features. But cloud services require to face the similar security issues and Security necessities; and we also can't be detached from the classical access control model concepts. For illegal Access harms, it often made on breakable ID verification and approval. The mainly causes consist of:

- No authentication or breakable authentication;
- To provide the authorized key and validation or confirmation information in plaintext. The system should accept a robust authentication procedure and provide secured transmission to prevent unauthorized access.

II STATUS OF CLOUD COMPUTING

Less initial investment
At the start, any business has to get the complete structure that wants for starting to run an assignment. It suggests that lots of expense in PC setup. If this business has all the in-house it implies that it ought to get few servers and personal pc powerful sufficient to help all the requiring of the business. If this business starts to usage some services within the cloud, it will cost less cash during this organization and capitalize it in different regions of the plan.

Costs reduction
As of expense by requirement, simply fee what's being employed, and since it's not essential to own establishments targeted on the upkeep and capability of the organization or package that's employed by cloud computing.

New functionalities and actualizations
The code informs area unit monitored by the supplier of the service, this supplier are going to be fascinated by actualize all the merchandise that they provide as shortly as doable to draw in additional purchasers. That the organization don't

ought to be disturbed regarding these items and don't would like special staff centered in this. [5]

Organization focused in business
Organization can emphasis their energies a lot of in business space and not most within the technical one. The main aim of any organization should be cost effective services and products with quality.

Access to data
As this services are net centered it's easy to right to use to any or all info of any other party or to his info through each straightforward stratagem with net affiliation, thus it's terribly suitable for that parties that have various access points. Specialists regarding cloud computing recognizes next points as potential issues regarding the utilization of cloud computing. [6]

Availability of Service
There's a giant obsession within the clients of cloud computing, it's however trustworthy is the service, as a result of the enterprises desires information and alternative services twenty four hours day. Suppliers cannot full assurance of sharing however their degrees of obtain ability of service are high. Supplier's deals an agreement, SLA (however generally it's tough to grasp however critics are often lose a service for some time.

Data Lock-in:
The application interface of cloud computing are still no standardized, therefore it's tough to share info among suppliers in simplified method. additionally it's tough to usage in similar method 2 completely other suppliers and additionally signify consumer see that suppliers have additional power than themselves, as a result of if enterprise needs to alter of supplier it'll be tough to alter all services and knowledge and this generates, making disbelief in purchasers. [6]

Low responsibility within the security of data
Info is that the one amongst the foremost valued vigorous in enterprise, therefore it's an awfully necessary call the way to have it. It's traditional to assume that have this info outer of the business will be a drag. Additionally managers of businesses are sometimes conventional during this reasonably selections therefore it's still a drag. Commonly organizations arrange to find non crucial info within the cloud and save the private one hosted within the business.

Low performance/Points of failure
The speed and latency problem of the networks is a blockage simply. The throughput of our system is affected especially within the IaaS deal, wherever we want huge volume of knowledge transmission. Additionally we have a tendency to get 2 a lot of completely different points of letdown: the affiliation of the individual business and also the affiliation of the supplier.

Difficult to customize the application:
Services provided within the open cloud are centered to many clients, don't seem to be centered specifically issues, simply centered generally resolutions and frequently don't disclose a lot of personalization. It describes it's exhausting to search out focused applications related to the in-house code arcade wherever we will results to the majority requirements.

III ISSUES AND CHALLENGES

DATA SECURITY

The procedure of keeping data on the cloud and access that data from the cloud, the main things are intricate: the customer, server, and network among them [7]. These three components must keep robust security to make mandatory of data security. User is liable for guaranteeing that no another party can approach to the model. In this case when consider the security issue of cloud storehouse, our motive is more about another two components i.e. server and the network among server and client.

All cloud server storing sources are handled by high achievement and high accessibility store house capacity system. Several cloud results work on personal hard-disks from the host network, which describes any computational or stowage let-down can cause in down period and probable data loss. As cloud servers are self-directed, if there occurs any server crash in kept data, these can be endangered against in-house and external attacks.

DATA INTEGRITY AND CONFIDENTIALITY

Confidentiality and uniformity of data can be confirmed on the both adjacent of server i.e. server side and user side. Communication among user and server must be through a protected network, means the data should be private and uniformity during the transmission over server and user. Several protocols such as SSL [8] to attain to a secure communication.

DATA AVAILABILITY

Availability of resources as well as stored data and information to the server is confirmed, and then the server should always guarantee that kept information are available for clients [7]. The final component of significance also is the network among the server and the user.

DYNAMIC ENVIRONMENT

Data used on cloud computing should be in a dynamic auditing structure. The central theory in this self-motivated atmosphere is that all regulated and flexible setup should have lively action such as updation, add, and remove. The cloud podium which has virtualized circumstances also should have some definite autonomous environs.

IV RELATED WORK

Cloud computing [8] uses three supply models by which different kinds of services are delivered to the end user or client. There are three service models SaaS, PaaS and IaaS which deliver structure resources, application platform and software as services to the user. These service models also place a different level of security requirement in the cloud environment. These issues [9] are:-

- Data security
- Network security

- Data locality
- Data integrity
- Data segregation
- Access control/ Data access
- Authentication and authorization
- Data confidentiality
- Web application security
- Data breaches
- Virtualization vulnerability
- Availability
- Backup
- Identity management and sign-on process.

M. Raykova [11] proposed a technique for access control to ensure security in cloud computing ; in this work author proposed a two-level access control phenomena that syndicates coarse-grained access control enforced at the cloud, which permits to get satisfactory computational overhead and at the same time limits the information that the cloud learns from his partial view of the access rules and the ac- cess patterns, and fine-grained cryptographic access control enforced at the user's side, which provides the desired expressiveness of the access control policies.

In UCON; C. Danwei et al. [12] proposed a framework of security on the basis of six parameters Subjects, Rights, Objects, Authorization, obligations, conditions to access the service by user or client. This parameter work as a digital certificate or policies for access control.

Provide a service through these parameters may increase the level of security, but these policies and certificate can easily detected by the adversaries or unauthorized user as well as the group of users(or servers).

V PROPOSED WORK

Among all security and management necessities of cloud computing, access control is one of the important requirements in order to its security and handle its dynamic nature avoid securely management issues. In this work we will introduce a model which provide the security through parameters (certificates and policies) by KP-ABE (Key Policy Attribute based Encryption); it is a public key security mechanism primitive for one-to-many connections. In KP-ABE, data are related with attributes for every which a public key element is determined. The encrypt rallies the group and subset of attributes to the original message by encrypting it with the equivalent public key elements. Each client is consigned an access configuration which is typically describe as an access tree over data attributes, i.e., inner nodes of the access tree are threshold gates and leaf nodes are related with attributes. Client secret key is described to replicate the access configuration so that the client is capable to decode an encrypted message if and only if the data attributes fulfill his access arrangement.

In this work we used to attribute for security and maintenance of the data:

1. Subject
2. Object

Subject is a unit which is about to rights of using object. Subject defies extensively, it may be the consumer gathering, the client himself, or may also be a workstation, card mechanism, wireless terminal, and even may be a platform or process application. Object is an entity which receives the visit of Subject. Object also has extensive significances, and it may be info, files and records used in workflow scheme, or may be hardware on the network and wireless communication terminals.

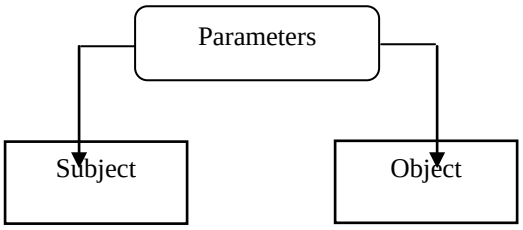

Figure 1: Parameters of certificate or policies.

In this work KP-ABE is also used to enhance the security of these above parameters. KP-ABE associates with set of attributes. Here the two parameters have the attributes subject and object. Subject attribute classifies the leading abilities and structures of subject; for ex identity, client group, part, membership, and dimensions list and security level. Object Attribute identifies the important information of object attributes contain security label, associations, type and storage lists and so on.

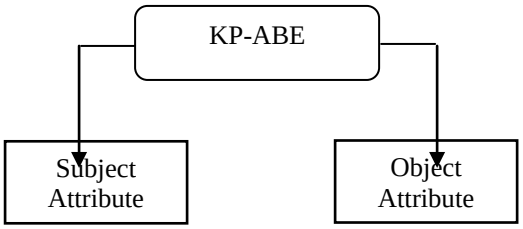

Figure 2: Subject and Object attribute.

Suppose S is the collection of all the attribute of Subject of database:

$$\mathbf{S= \{S_1, S_2, S_3, S_4 \ldots\ldots\ldots\ldots S_m\}}$$

Similarly O is the collection of all attribute of Object of database:

$$\mathbf{O= \{O_1, O_2, O_3, S_4 \ldots\ldots\ldots\ldots O_n\}}$$

So, the universe of all the attribute is U:

$$\mathbf{U= \{S, O\}}$$

In this work, rules and certificate may be described over attributes applying AND, OR and (k, m+n)-threshold gates means k out of m+n attributes (m for subject and n for object) have to be present.

For instance, let us assume that {A, B, C, D} are subset of universe U of subject and object attributes.

$$\mathbf{U= \{}A\mathbf{,}\ B\mathbf{,}\ C\mathbf{,}\ D\mathbf{\} = \{S, O\}}$$

And if first user/client obtains a key to attributes {A, B} and client or second user to attribute {D}. If an encryption is coded with respect to the policy $(A \wedge C) \vee D$, then second client will be capable to access or decode, while first client

will not be capable to access. From the above encryption we provided security of data and control a huge data for different authenticated users and prevent from unauthorized access of that data or services.

VI RESULT ANALYIS

For relevancy of work, the result of proposed method is compared with previous model. The results clarify that the proposed work helps in increasing the security on cloud. Therefore the proposed work has higher security and may increase overhead. The comparison of the UCON model [13] [14] [15] and proposed work on the basis of below parameters is depicted in table 1.

Parameters	Classical model	Proposed Model
Efficiency	Average	High
Computational Overhead	Average	Low
Fine grain Access Control	Average	High
Collision Resistant	Average	Average
Cloud Security	Average	High
Key Size	Constant	Linear
Data Sharing	Allow	Allow

VII CONCLUSION

In this paper the architecture that uses some certificate and policies with KP-ABE algorithm for better data storage is proposed, which is an enhancement over data storage. The proposed method offers framework that uses certificate as a subject, object, conditions etc. with key policy attribute base encryption for authorization. These policies have attribute like identity, term bonding, duration level etc. on the basis of these attribute the provider (server) provides the different service to each individual client.

The proposed work can be further elongated to improve a toolbar, which has the all package of storage capability, service and authorized user access only those service from this package which they are eligible or permit for.

REFERENCES:-

1. Y. G. Min, Y. H. Bang, "Cloud Computing Security Issues and Access Control S5.olutions," Journal of Security Engineering, vol.2, 2012.
2. E. Yuan and J. Tong, "Attribute Based Access Control (ABAS) for web Services," Conference on Web Service, IEEE, 2005.
3. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Springer-Verlag Berlin Heidelberg -2009.
4. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.
5. M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol 24, no 1, Jan 2013.
6. Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure Computing, vol 9, no 6 NOV/DEC 2012.
7. B. S. Bindu, B. Yadaiah, "Secure Data Storage In Cloud Computing," International Journal of Research in Computer Science, Vol 1 Issue 1, pp. 63-73, 2011.
8. M. Zhou, Y. Mu, W. Susilo, M. H. Au, "Privacy-Preserved Access Control for Cloud Computing," IEEE International Joint Conference, 2011.
9. S. Subashini, V. Kavitha," A Survey on Security issues in Service delivery models of Cloud Computing," ELSEVIER, 2011.
10. L. Wang, D. Wijesekera and S. Jajodia, "A logic based framework for attribute based access control. Proceeding of ACM workshop on formal methods in Security Engineering. pp. 45-55, ACM press.2004.
11. M. Raykova, H. Zhao, and S. M. Bellovin, "Privacy Enhanced Access Control for Outsourced Data Sharing," Columbia University, Department of Computer Science,New York.
12. C. Danwei, H. Xiuli, and R. Xunyi, "Acess Control of Cloud Computing service based on UCON," Nanjing University of posts & Telecommunications, Springer 2009.
13. S.Yu, C.Wang, K.Ren, W.Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Journel from Illinois Institute of Technology.
14. A. Pimlott and O. Kiselyov, "A Logic Based Trust Management System," Proceeding of 8th international symposium on Functional and Logic Programming, Springer, Japan. 2006, pp. 130-144.
15. E. Damianiet al., "New Paradigm for Access Control in Open Environment," Proceeding of 5th IEEE International Symposium on Signal Processing and Information.2005.

16. P. Bonatti and P. Samarati, "A unified framework for regulating access and information release on the web," Journal of computer Security. 10(3): 241-272.2002.

17. E. Yuan and J. Tong, "Attribute Based Access Control (ABAS) for web Services," Proceeding of IEEE Conference on Web Service.

18. V. Welch et al., "Attributes, Anonymity and Access: Shibboleth and Globus Integration to Facilitate Grid collaboration," Proceeding of 4th annual PKI (R and D) workshop.2005.

19. T. Barton et al., "Identity Federation and Attribute Based Authorization through the Globus Toolkit," Shibboleth, Gridshib and My Proxy. Proceeding of 5th Annual PKI (R and D) workshop.2006.