A Technical Review on Access Control in Cloud Computing

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
The usage of web and innovative technologies today, for professional and for personal, is already a part of lifestyle. Any information is accessible at anywhere within the globe at any time. Few years ago that wasn't possible. Cloud computing is an advanced emerging technology. Cloud computing is an efficient solution for the easiest and fastest storage and retrieval of data. Cloud service is centered on Web Service area, and it will face all types of security issues comprising what Web Services aspect. The central problem in cloud computing is security.In this paper we discuss access control in cloud computing for security aspect. This paper offers a comprehensive analysis of several methods of access control in cloud computing based on different domains with their merits and demerits. A brief evaluation has been prepared among the different access control methods based on certain factors.

Keywords—Cloud computing. Access Control; Data authenticity; Data integrity.

INTRODUCTION

The usage of web and innovative technologies today, for commerce and for these clients, is even now a part of living. Any information is accessible at anywhere within the globe at any time. Few years ago that wasn't probable [1]. Nowadays it have increased lots of projections of right to use to public and private data like web speed access or the preparing of moveable dispositive that allow the joining to web from virtually all over. Today lots of person's are retrieving their mail on-line through webmail shoppers, writing willing documents victimization net browsers, making computer-generated photo album 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 this 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 universal source where client request to preserve all his data with security measurement through this various application, program and computational models can raise complete earnings via this technology without any confined physical storage device and server for his data storing. These amenities and services are usually scattered into three types 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 systems 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 TECHNOLOGY RELATED

In this section we are going to explain some technologies that are linked to cloud computing.

WEB SERVICES

It's explained earlier that cloud computing it's primarily based within the provider of services, however what's specifically a service and the way it works? ordinarily 2 applications written in several languages and dead in several in operation systems aren't able to communicate between them, however exists a bunch of protocols and standards for exchanging data between completely different applications, notwithstanding within which language written or within which package running. This can be extremely helpful, for instance over web, once we don't savvy is enforced as application running on the net.

This can be attainable due to organizations like OASIS (Organization for the Advancement of Structured data

Standards) and W3C (World Wide net Consortium). This communication relies in plain text. therefore it‘s not an equivalent economical as different reasonably communication like CORBA or RMI. (Remote invocation method) the various technologies used for this communication are:

XML (EXTENSIBLE MARKUP LANGUAGE)
It’s a Meta language supported on labels. It’s terribly structured and permits to totally different applications or systems to speak between them. Because it is claimed within the name is extensile, that it implies that it permits shaping new labels simply.

SOAP (Simple Object Access Protocol)
It’s a protocol that describes how 2 objects of dissimilar processes can share info through XML messages.

WSDL (Web Services Description Language)
Centered on XML and it’s the open interface in the sphere of web services. It defines all the services that are present in one location and the way to network with them.

UDDI (Universal Description, Discovery and Integration)
It’s a directory of all internet services that are present in Internet, it was an industrial initiative but today it’s not actually used. It’s written in XML.

WS-Security (Web Service Security)
It’s an addition to SOAP to smear security to web services.
Cloud computing security
It‘s a collection of policies regarding the safety within the cloud targeted on laptop, network and principally info protection. These policies are about:

- Information of 1 user have be entirely isolate from information of another and it got to be affected firmly within the cloud.
- Use of identities.
- Physical infrastructure needs to be utterly secure and also the access to the info wants identification.
- Access to information got to be continuously out there for the users, it can‘t happen that one user cannot access to his own information at one moment.
- All the services delivered within the cloud got to be secure.
- All wise information got to be encrypted.

DATACENTERS
The enterprises that require to storage and method lots of data use usually data centers. This information centers typically are racks within rooms dedicated to it with special conditions. Datacenters should embrace heap of many security policies and redundancies of knowledge, power and communication provide and ought to be in distinct conditions, like temperature, humidity, etc.

CLOUD STORAGE
It‘s the virtualization of the storage of info mistreatment through net and frequently by third elements. There are several corporations that have immense information centers that permit to others to store on them their date by mistreatment virtual servers and storage pools. That the shopper sees their files that are organized among in several locations within the information center, as if they were set physically within the same place. This can be terribly helpful as a result of enterprises don‘t need to be troubled regarding the infrastructure of their information center however conjointly they pay money for what proportion information they're storing there

VIRTUALIZATION OF COMPUTERS
Virtualization is an abstraction of the resources of a machine among the hardware and therefore the software package, creating a virtual version of a resource being doable to share it. Regarding virtualization of computers, software package simulates a whole machine within another one. unremarkably is an software package that's dead as if it had been the sole one running within the pc, however that‘s not real as a result of it’s running in conjunction with alternative operation systems and don’t have all the resources of the machine, simply a section of them.

That software package have to be compelled to manage the principal resources of pc, CPU, RAM, storage and network and therefore the system has got to be ready to permit all users work along. This virtualization will be: Complete, during this case the hardware simulated is enough to run standard software package for an equivalent machine as if it had been running utterly normal. Partial, It‘s a fractional virtualization, share resources and host procedures, Therefore it‘s a virtualization of the house of addresses. Virtualization for O.S. inside one O.S inside another one by employing a virtual machine. The O.S virtualized isn't as potent because it might be if it had been the sole one running. With this selection we will run totally different O.S within the same machine.

GREEN IT
It’s the style to maximize the potency of the procedure resources to attenuate the environmental impact. Additionally includes the readying of ecologic merchandise. Some technologies enclosed in Green IT are cloud computing, grid and datacenters. Cloud computing is a component of inexperienced IT as a result of with the usage of dynamic resources the enterprises lessen the energetic consumption.

GRID
Infrastructure that integrates totally different systems from different establishments like if it absolutely was only 1 (computers, networks, databases, etc.) permitting the collective use. This can be the distinction with cloud computing, as a result of in cloud all the infrastructure is managed by one organization though every cloud will use dynamically others clouds too.

VIRTUAL APPLIANCE
It‘s a virtual machine compressed in an exceedingly file, with a program like Xen or VmWare it‘s doable to run this Virtual Machine within the host. Typically this VM are created with an operative system and a few applications put in for one in every of succeeding purposes:

- Virtual servers.
- Routers and Firewalls
- Observance

III ISSUES AND CHALLENGES

There are many issues related to cloud computing but security is the main issues among them like data availability, environment updation, cost etc.

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 [6]. 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 storehouse 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. The complexity of security risks in a complete cloud environment is illustrated in Fig. 1.

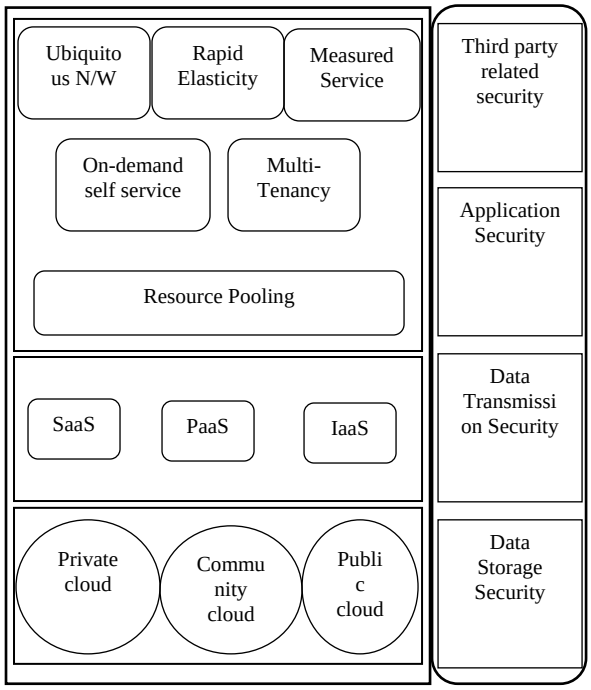

Figure 1: Complexity of security in cloud environment.

IV RELATED WORK

Cloud computing [6] 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 [6] 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.

Y. tang et al. [7] proposed a method for access control in cloud computing name as FADE. The model [7] offers fine-grained access control and guaranteed identification for outsourced data or service on the cloud. But this structure is not successfully applicable because if the data holders and service providers are in different zone, then it behave as anon-effective policy.

Another method for access control is HASBE which is presented by Z. Wan et al. [8]. The key limitation of this work [8] is that it is not flexible related to other works.

S. Yu et al. proposed a model [9] for access control in cloud computing. In this method [9], author used KP-ABE (Key Policy Attribute Based Encryption) and PRE(Proxy Re-Encryption) algorithm. This approach is not scalable due to the overhead of encryption and decryption.

Y. Zhu et al. [10] proposed an approach for time-based access control in cloud computing. This method [10] is only appropriate to systems in which data proprietors and the service providers are within the similar trusted field. Another main approach is described by M.Li et al. But it is very costly scheme.

M.Zhou at al. proposed a model [12] for privacy-preserved access control for cloud computing in an International Joint Conference of IEEE TransCom-11. This model [12] also has some disadvantages. But here, in this structure, absence of flexibility and scalability make it as non-effective.

M. Raykova [15] 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. [16] 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. These 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 COMPARATIVE ANALYSIS

All the discussed techniques or model for access control in cloud computing have some benefits and drawbacks based on the method proposed or used by different authors. So, the comparison of all the approaches with respect to their advantages and limitations are shown in table.1.

Table.1 Comparative Analysis

Method/Model	Merits	Demerits
FADE[7]	Effective and Fine grain access control	Service owner and provider must be in same domain
HASBE[8]	Effective Access control	Minimum flexibility
KP-ABE[9]	Security increase due to encryption and decryption	High overhead due to the same encryption and decryption
Temporal Access[10]	Cost Effective access control	Service owner and provider must be in same trusted domain
Privacy Preserved[12]	Effective access control	Due to less scalability and flexibility effectiveness of this model become quite poor.
Two level Access control[15]	Coarse-grained access control	Desired expressiveness of the access control policies
UCON[16]	Cost effective and less overhead	Policies and certificate can easily detected

VI CONCLUSION

We have discussed certain approaches for access control in cloud computing centered on various fields. All models have some strong point and limitations, but the object of all the approaches are to provide better access control for users, provides, and owners in cloud computing in the aspect of security of data. A comparative exploration on the basis of certain stricturesand a brief comparison is being delivered between the all discussed methods.

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. 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.
7. 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.
8. Z.Wan, J.Liu, R.H.Deng, “HASBE:A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing,” IEEE Transactions on Forensics and Security, vol 7, no 2, APR 2012.
9. S.Yu, C.Wang, K.Ren, W.Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” Journal from Illinois Institute of Technology.
10. Y.Zhu, Hu, D.Huang, S.Wang, “Towards Temporal Access Control in Cloud Computing,” Arizona State University, U.S.A.
11. 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.

12. M. Zhou, Y. Mu, W. Susilo, M. H. Au, "Privacy-Preserved Access Control for Cloud Computing," IEEE International Joint Conference, 2011.

13. S. Subashini, V. Kavitha," A Survey on Security issues in Service delivery models of Cloud Computing," ELSEVIER, 2011.

14. 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.

15. M. Raykova, H. Zhao, and S. M. Bellovin, "Privacy Enhanced Access Control for Outsourced Data Sharing," Columbia University, Department of Computer Science, New York.

16. C. Danwei, H. Xiuli, and R. Xunyi, "Acess Control of Cloud Computing service based on UCON," Nanjing University of posts & Telecommunications, Springer 2009.

17. 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.

18. E. Damiani et al., "New Paradigm for Access Control in Open Environment," Proceeding of 5th IEEE International Symposium on Signal Processing and Information.2005.

19. 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.

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

21. 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.

22. 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.