Cloud Computing: Secure and Scalable Data Access Security Models

Anupama Prasanth
Lecturer
College of Computer Studies
AMA International University

ABSTRACT
Cloud computing has built up itself as a standout amongst the most famous advancements accessible presently. It has increased much veneration, yet with fast usage of cloud computing, the security factor has come to forefront. Organizations are pushing toward cloud computing for getting advantage of its cost lessening and versatility highlights. However cloud computing has potential risks and vulnerabilities. One of real obstacle in moving to cloud computing is its security and protection concerns. As in cloud computing environment data is out of client ownership this prompts extraordinary danger of information trustworthiness, information secrecy and information weakness and so on. Various security models have been produced to adapt to these security dangers. Our study aims at the various security models that were produced for securing information. The different well known security models of distributed computing like "The Cloud Multiple Tenancy Model of NIST", "The Cloud Risk Accumulation Model of CSA", "Jerico Forum's Cloud Cube Model" and "Multi-Clouds Database Model" have been reviewed in this paper.

General Terms
Cloud Security

Keywords
Cloud Security, Multiple Tenancy Model, Risk Accumulation Model, Jerico Forum's Model, Multi-Cloud Database Model.

1. INTRODUCTION
Cloud computing is an innovative paradigm which showed up worldview in 2006. It is actually transformed from parallel computing, distributed computing, utility computing and grid computing, and the developmental outcome of network storage, virtualization and load balance [1]. By combining a set of existing and new techniques such as Service-Oriented Architectures (SOA) and virtualization, cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet. The main idea of cloud computing is to build a virtualized computing resource pool by centralizing abundant computing resources connected with network and present the service of infrastructure, platform and software. This network that offers various computing resources is called "cloud" [2]. Successful examples are Amazon's EC2 and S3 [3], Google App Engine [4], and Microsoft Azure [5] which provide users with scalable resources in the pay-as-you use fashion at relatively low prices. For example, Amazon's S3 data storage service just charges $0.12 to $0.15 per gigabyte per month. When contrasted with building their own particular frameworks, users can spare their ventures fundamentally by moving organizations into the cloud. With the expanding improvement of cloud computing innovations, it is not hard to envision that sooner rather than later an ever increasing number of organizations will be moved into the cloud.

As promising as it seems to be, cloud computing is additionally confronting many difficulties that, if not very much settled, may obstruct its quick development. Information security, as it exists in numerous different applications, is among these difficulties that would raise incredible worries from users when they store delicate data on cloud servers. These worries start from the way that cloud servers are generally worked by business suppliers which are probably going to be outside of the put stock in space of the clients. Information privacy against cloud servers is consequently every now and again craved when users outsource information for capacity in the cloud. In some down to earth application frameworks, information classification is a security/protection issue, as well as of juristic concerns. For example, in healthcare application scenarios use and disclosure of protected health information (PHI) should meet the requirements of Health Insurance Portability and Accountability Act (HIPAA) [6], and keeping user data confidential against the storage servers is not just an option, but a requirement. Furthermore, we watch that there are additionally cases in which cloud users themselves are content suppliers. They distribute information on cloud servers for sharing and need fine-grained information get to control as far as which user (data customer) has the get to benefit to which sorts of information. In the medicinal services case, for instance, a restorative focus would be the information proprietor who stores a large number of social insurance records in the cloud. It would allow data consumers such as doctors, patients, researchers and etc, to access various types of healthcare records under policies admitted by HIPAA. To enforce these access policies, the data owners on one hand would like to take advantage of the abundant resources that the cloud provides for efficiency and economy; on the other hand, they may want to keep the data contents confidential against cloud servers.

One of the significant obstacles in moving to cloud computing is its security and protection concerns. As in cloud computing condition information is out of client ownership this builds the danger of information honesty, information classification and so forth. To decrease these dangers scientists have purposed numerous security models. This study will research security models that were created for securing information amid entire lifecycle of distributed computing. In next sections will present distinctive security models purposed for various security dangers

2. RELATED WORKS
Cloud computing gathers all the resources and oversees them naturally through programming. The recorded information and present information are incorporated to make the collected data more exact. Along these lines cloud computing gives more smart support of the users. The users are not made a big deal about how to purchase a server or solution. Rather they can purchase the computing resource on the web as indicated by their need. However cloud computing rise as

promising innovation so as to give the service remotely. Be that as it may, there are numerous security issues in cloud computing. For instance in February, 2010, the Amazon organize have benefit, S3 (Simple Storage Service) was broken down for 4 hours. This made individuals consider the security of cloud computing once more. Since Amazon gives S3, it has pulled in a ton of business visionary on Web 2.0 put their site on the server farm of Amazon to spare a substantial equipment venture [16]. So the administration of cloud computing is not steady and authentic. Security is as yet a noteworthy worry in distributed computing and one of the reasons that cloud computing is still not conceded by the clients.

As a significant research area for system protection, data access control has been evolving in the past thirty years and various techniques [7]–[10] have been developed to effectively implement fine-grained access control, which allows flexibility in specifying differential access rights of individual users. Traditional access control architectures usually assume the data owner and the servers store the data in the same trusted domain, where the servers are fully entrusted as an omniscient reference monitor [11] responsible for defining and enforcing access control policies. This assumption however no longer holds in cloud computing since the data owner and cloud servers are very likely to be in two different domains. On one hand, cloud servers are not entitled to access the outsourced data content for data confidentiality; on the other hand, the data resources are not physically under the full control of the owner. For the purpose of helping the data owner enjoy fine-grained access control of data stored on untrusted cloud servers, a feasible solution would be encrypting data through certain cryptographic primitive(s), and disclosing decryption keys only to authorized users. Unauthorized users, including cloud servers, are not able to decrypt since they do not have the data decryption keys. This general method actually has been widely adopted by existing works [12]–[15] which aim at securing data storage on untrusted servers.

To enhance security of cloud many models have been purposed. Client might want to know which security conspire they ought to actualize for securing our information. Correlation of these security plans have likewise been finished by numerous analysts, for example, Farzad Sabahi talk about numerous security issues to distributed computing against these issues. [17] .

In this section we will introduce different security models which were purposed by different researchers. We will also tell about each security model that in which layer it works.

3. CLOUD COMPUTING SECURITY

Cloud security alludes to a wide arrangement of approaches, innovations, and controls conveyed to ensure information, applications, and the related infrastructure of cloud computing. Cloud computing and storage provides users with abilities to store and process their information in third-party servers. So the major issues related to security are Trust and Identification of Threat.

3.1 Trust

Trust in a cloud environment depends intensely on the model in which the data administration and applications is outsourced and designated out of the owners strict control. In customary designs, trust was authorized by a productive security arrangement, which tended to limitations on capacities and stream among them, requirements on access by outer frameworks and enemies including projects and access to information by individuals. In a cloud deployment, this recognition is completely darkened. On account of open or group mists, control is appointed to the association owning the framework. When conveying on an open cloud, control is relieved to the framework proprietor to implement an adequate security strategy that ensures that proper security are being performed to guarantee that hazard is reduced. This presents various dangers, as basically security is identified with believing the procedures and figuring base executed by the cloud owners. It is essential to separate between sending models, as a private cloud, where the foundation is worked and overseen on start by a private association, does not present extra extraordinary security challenges, as trust stays inside the association. In such a circumstance the infrastructure owner remains the information and process owner. The development of cloud service models, is required to prompt a deconstruction of the service benefits as they are now conveyed in existing ""shut"" service provisioning situations [23].

3.2 Security Identification of Threat

Basically securing an Information System (IS), includes recognizing one of a kind dangers and difficulties which should be tended to by executing the appropriate countermeasures. Security all in all, is identified with the imperative parts of privacy, respectability and accessibility; they in this way progress toward becoming building blocks to be utilized as a part of outlining secure frameworks. These imperative parts of security, apply to the three general classes of advantages which are important to be secured, information, software and hardware resources. The cloud infrastructure proposes remarkable security challenges which should be considered in subtle elements are Confidentiality and privacy, Integrity and Availabilty.

3.2.1 **Confidentaility:** Confidentaility alludes to just authorized parties or systems being able to get to secured information. The danger of information bargain increments in the cloud, because of the expanded number of parties, gadgets and applications included, that prompts an expansion in the quantity of purposes of get to. Assigning information control to the cloud, contrarily prompts an expansion in the danger of information trade off, as the information ends up noticeably available to an expanded number of gatherings. Various concerns rise in regards to the issues of multitenancy, information remanence, application security and protection [24]

3.2.2 **Integrity:** A key part of Information Security is honesty. Honesty implies that advantages can be altered just by approved gatherings or in approved ways and alludes to information, programming and equipment. Information Integrity alludes to protecting information from unauthorized deletion, change or creation. Dealing with an element's permission and rights to particular undertaking assets guarantees that profitable information and services are not mishandled, abused or stolen. By averting unapproved get to, associations can accomplish more noteworthy trust in information and system uprightness. Also, such components offer the more noteworthy perceivably into figuring out who or what may have modified information or system data, possibly influencing their respectability (responsibility). Approval is the component by which a system figures out what level of get to a specific verified client ought to need to secured assets controlled by the system. Because of the expanded number of elements and get to focuses in a cloud

situation, approval is significant in guaranteeing that lone approved elements can communicate with information.

3.2.3 Availability: Availability alludes to the property of a system being available and usable upon request by an approved substance. System accessibility incorporates a system capacity to bear on operations notwithstanding when a few authorities misbehave. The framework must be able to proceed with operations even in the likelihood of a security additionally equipment being rupture. Accessibility alludes to information, programming. accessible to approved users upon request. Utilizing users from equipment framework requests, creates a substantial dependence on the pervasive system's accessibility.

4. CLOUD COMPUTING SECURITY MODELS

Information security and security assurance are the essential targets of the cloud users. The cloud service providers must neither unveil nor release the users's private information nor ought it to itself break down users's information and jab into the protection. For instance there might be a mystery arrangement marked by two associations about their clients and their benefit techniques which ought not end up plainly open. The protection and information security contains life cycle of creation, stockpiling, use, sharing, refreshing and destroying of information. The most extreme critical issue of present situation is security of cloud computing and to tackle it there is a need to manufacture cloud computing security models also, break down the key advances utilized as a part of these models. [18]

4.1 The Cloud Multiple-Tenancy Model of NIST

The huge practical normal for cloud computing is Multiple-tenancy.[19] It permits cloud providers presently running different applications in physical server to offer cloud services to clients. The physical server partitions distinctive client's requests in into equivalent segments and procedures them with virtualization procedure. Sharing and isolation are the key elements of virtualization and is the essential innovation of distributed computing. By permitting running of different virtual machines (VMs) in a physical machine, virtualization empowers distinctive clients' applications to share computing resource, for example, memory, stockpiling, processor, and I/O among, and enhances the use of cloud assets. By facilitating diverse clients' applications into various virtual machines, virtualization can isolate form fault, virus, and intrusion from other virtual machines and hardware, and reduce the damage caused by malicious applications. The innovation challenges endured by various occupancy model are design expansion, information separation, setup selfdefinition, also, execution customization. Information segregation implies that the business information of various clients don't mediate commonly. Design expansion implies that different tenure ought to give a fundamental structure to execute high adaptability what's more, versatility. Design self definition implies that diverse clients' separate requests distributed computing ought to be bolstered on its administration stage setup. By Performance customization it is implied that diverse requests of numerous clients ought to be proficiently met under various levels of workload. Numerous tenure model effects in various routes in various cloud sending models. Different occupancy model of distributed computing executed by virtualization innovation offers a technique to fulfill distinctive client requests on governance, division, security, SLA , isolation and charging/chargeback and so forth [19]

In simple, utilization of same applications or assets in the meantime by various clients that could conceivably have a place with same association can be named as Multi-occupancy. From a supplier viewpoint, multi-tenure can be portrayed as a structural and configuration way to deal with take into account the requirements of various clients and to empower economies of scale. [20]

4.2 The Cloud Risk Accumulation Model of CSA

To inspect the security dangers postured by cloud computing it is crucial to comprehend the layer reliance of cloud service models.[19] IaaS is the fundamental establishment layer of all cloud service, PaaS is based upon IaaS and SaaS is based upon PaaS, so there is inherited among the service capacity of various layers in cloud computing. The security dangers of cloud computing is additionally acquired among various service layers like cloud service capacity legacy.
Maximum extensibility is offered by IaaS. It gives irrelevant security capacities and abilities with special case to its own particular framework. IaaS in control clients with the security of programming applications and substance, working frameworks, and so forth. The ability of creating modified applications for clients in view of the PaaS platform is offered by PaaS. It gives more extensibility than SaaS, at the cost of reducing those accessible particular elements of SaaS. Essentially, PaaS offers greater adaptability to clients for executing extra security.

The minimum user extensibility is offered by SaaS, yet it shows the most incorporated service and the most astounding coordinated security among three service layers. Cloud service providers assume responsibility of greater security obligations in SaaS, and clients needs to pay for little security endeavors on the SaaS stage.

Lower the service layer that a cloud service provider lies in, the greater service obligations and security capacities that a client is responsible for is one of the essential feature for cloud security design. Cloud specialist organizations need to fulfill the requests on SLA, security, screen, consistence and obligation desire and so on in SaaS. In PaaS and IaaS, the above requests are dealt with by clients, and cloud service providers are in charge of the accessibility and security of elementary service [19]

4.3 Jerico forum's cloud cube model

Jerico forum's cloud cube model [4] is a perception of blend of deployment models, cloud service models of cloud computing, the attributive detail of administration and proprietorship and physical area of assets, proprietor and chief of assets Different model parameters utilized as a part of cloud cube model is as per the following:

Internal/External: It portrays the physical area where real information is stored. If information is stored inside the limits of proprietor of the information, then the estimation of model parameter is internal and vice versa. For instance, the server farm of a private business organization cloud is internal, and the data center of Amazon's SC3 is external. The cloud with internal information storage is not really more secure than the one with external information storage. The blend of internal and external information storage might be best suitable solution for more secure usage model.

Proprietary/Open: The responsibility for innovation, interface and service and so forth is best portrayed by this parameter. The level of interoperability, i.e. the capacity of changing information from a cloud methodology to other cloud methodology with no requirement, the convenience of information and application between exclusive framework and other cloud modalities is demonstrated by this parameter. At the point when a cloud service provider holds the responsibility for giving cloud administrations, it is named as exclusive, henceforth the operation of cloud is restrictive and clients can not exchange their applications among various cloud specialist organization easily. The innovations utilized as a part of open cloud are for the most part open and uniform, which means more accessible specialist organizations and less requirement on information offer and fuse with business partners. unprove however most, open cloud can advance effortlessly and viably the consolidation between numerous associations.

Parameterized/De-parameterized: To show the "architectural mindset" of security insurance, i.e. regardless of whether a client's application is inside the conventional security limit or outside this modular parameter is utilized. Parameterized is the point at which a client's application works inside conventional IT security limit signaled by firewall that obstructs the joining of distinctive security zones. Actually, clients running a few applications within security zone can extend/shrivel their application edge to/once more from outside cloud condition by virtual Private Network. De-parameterized is the blur method for customary IT security limit and the introduction of a client's application operation. For the security insurance of de-parameterized condition, Jerico Forum utilizes the meta-information and instruments in their precepts and Collaboration Oriented Architectures. Structure (COA) to exemplify information of client.

Insourced/Outsourced :This model parameter is utilized to characterize the fourth measurement that has two states in each of the eight cloud shapes: Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO). Insourced can be characterized as cloud benefit displayed by an association's own particular representatives, and Outsourced can be named as that cloud benefit which is displayed by an outsider. This is a arrangement issue a business one however not a specialized or engineering choice. [19] [21] [20]

4.4 Multi-Clouds Database Model

Multi-Clouds Database Model [22] presents cloud with database storage in multiclouds service provider. It is unique in relation to Amazon cloud benefit which gives solitary distributed storage information. MCDB demonstrate does not defend security by single cloud; rather security and protection of information will be given by executing multi shares system on multi-cloud suppliers. Thus, it decreases the negative impacts of single cloud, lessens the security dangers from noxious insider in cloud computing condition, and limits the negative effect of encryption methods. MCDB gives security and protection of client's information by imitating information among a few clouds and by utilizing the mystery sharing methodology. It manages the database administration framework (information source) to oversee and control the operations between the customers and the cloud specialist organizations (CSP). At the customer side, this sends information request to server or example, for example, in Amazon in CSP. The information source stores the information in the cloud side which should be confided in cloud, additional to guaranteeing that the protection of any query that the customer has made and for the security of the customer stored information. An issue happens when we can't ensure cloud is a confided in trusted service. [22]

5. COMPARISON ANALYSIS

In this section analysis and evaluation of the cloud computing security models has been done on the basis of following parameters: Trust, Confidentiality, Integrity, Availability and Technology used. The comparison and analysis of these parameters are shown in Table1 .

Table 1: Comparative Analysis

MODELS	TRUST	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	TECHNIQUES
Cloud Multi-Tenancy Model	Medium	very different access control policies	very different access control policies	Resources are shared among various users	Virtualization
Cloud Risk Accumulated Model	Medium	customers possess more flexibility to implement additional security	demands that customers take charge of the security of operating systems, software applications and contents etc	cloud service provider is only responsible for the availability and security of elementary services such as infrastructure component and underlying platform	Relationship among SaaS , IaaS and PaaS
Jerrico form's Cloud Cube Model	High	Organizations looking to procure cloud services must develop the ability to rapidly set up legally binding collaboration agreements, and to close them just as quickly once they become unnecessary.	Figuration description of resource owner , controller , location , service and deployment mode	Figuration description of resource owner , controller , location , service and deployment mode	Cloud in Cube Form
Multi-Clouds Database Model	Highly trustable	impossible to corrupt the data since it is replicated among different clouds; hackers need to retrieve all the information from cloud	users should compute the digest of data by using hash-based message authentication	Stores the information on multiple clouds	Data Replication

6. CONCLUSIONS AND FUTURE WORK

Cloud computing is the up surging innovation which is generally holding entire of the data business. The four models have been overviewed and analyzed. It has been inferred that Jerico Formu's Cloud Cube Model and Multi-Clouds Database Model are more secure in contrast with The Cloud Multiple-Tenancy Model of NIST and The Cloud Risk Accumulation Model of CSA. It has been examined that Multi-Clouds Database Model has less pernicious insiders among the other looked at models. As the future perspective work can be carried on to give more secure distributed computing security model to enhance the innovation utilized, approval, security and malicious insiders.

7. REFERENCES

[1] Vaquero L.M., Rodero-Merino L, Caceres J., Lindner M. A break in the clouds: towards a cloud definition. In: ACM SIGCOMM, editor. Computer communication review 2009. New York: ACM Press; 2009. p. 50–5.

[2] Boss G, Malladi P, Quan D, Legregni L, Hall H. Cloud computing, 2009. http://www.ibm.com/developerswork/ websphere /zones/hipods/ library.html.

[3] Amazon Web Services (AWS), Online at http://aws. amazon.com.

[4] Google App Engine, Online at http://code.google.com/appengine/.

[5] Microsoft Azure, http://www.microsoft.com/azure/.

[6] 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/ admnsimp/pl104191.htm, 1996

[7] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. of NDSS'01, 2001.

[8] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. of SP'02, 2002.

[9] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. of SP'03, 2003.

[10] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. of CCS'05, 2005.

[11] J. Anderson, "Computer Security Technology Planning Study," Air Force Electronic Systems Division, Report ESD-TR-73-51, 1972, http://seclab.cs.ucdavis.edu/ projects/history/.

[12] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable secure file sharing on untrusted storage," in Proc. of FAST'03, 2003.

[13] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. of NDSS'03, 2003.

[14] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS'05, 2005.

[15] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proc. of VLDB'07, 2007.

[16] ZHANG, S. et al. Cloud computing research and development trend. Future Networks, 2010. ICFN'10. Second International Conference on, 2010, IEEE. p.93-97.

[17] SABAHI, F. Cloud computing security threats and responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, 2011, IEEE. p.245-249.

[18] Su Qinggang; Wang Fu; Hang Qiangwei. (2012). Study of Cloud Computing Security Service Model," Engineering and Technology (S-CET), 2012 Spring Congress on, vol., no., pp.1,4, 27-30.

[19] Che Jianhua, Duan Yamin, Zhang Tao, Fan Jie. (2012). Study on the security models and strategies of cloud computing. 2011 International Conference on Power Electronics and Engineering Application. Procedia Engineering 23 (2011) 586 – 593.

[20] Hopkins Hupert. (2012). Securing the Cloud. diebold.

[21] Chang, V.; Bacigalupo, D.; Wills, G.; De Roure, D. (2010). A Categorisation of Cloud Computing Business Models. Cluster, Cloud and Grid Computing (CCGrid). 2010 10th IEEE/ACM International Conference on , vol., no., pp.509,512, 17-20.

[22] AlZain, M.A.; Soh, B.; Pardede, E. (2011). MCDB: Using Multi-clouds to Ensure Security in Cloud Computing. Dependable, Autonomic and Secure Computing (DASC). 2011 IEEE Ninth International Conference on , vol., no., pp.784,791, 12-14.

[23] K. Tserpes, F. Aisopos, D. Kyriazis, T. Varvarigou, Service selection decision support in the Internet of services, in: Economics of Grids, Clouds, Systems, and Services, in: Lecture Notes in Computer Science, vol. 6296, 2010, pp. 16–33. doi:10.1007/978-3-642-15681-6_2

[24] Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010.