Security and Scalability Measurement of Distributed Databases of Cloud Computing

Amudha T1, Sumithra Devi K A2, Saravanan K3

1 Research Scholar, Dept of Computer Science, PRIST University, Thanjavur, 613 403, Tamilnadu, India.
2 Department of Information Science & Engineering, DAE&IT, Bangallore, 560080, Karnataka, India.
3 Dean, Faculty of Computer Science, PRIST University, Vallam, Thanjavur, 613 403, Tamil Nadu, India.

Abstract
Cloud computing is a technique that has great capabilities and benefits for users. Cloud character support many organizations to move to this technology. But many considerations face the transmission process. Cloud computing is a promising computing paradigm which allows distribution of services from a pool of resources. The services are required by the clients through on-demand via pay and use method. The greatest utilization of resources and maximum profits with scheduling is the main goal of the cloud service providers. The major issue in cloud computing is the scheduling of services with improved global throughput and job scheduling. Since cloud computing is a service based one, the performance evaluation is an important criterion to be dealt. In this paper, we propose a priority based to evaluate the services leased by the cloud service providers. The services are considered to be SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).

Keywords: Cloud computing, SaaS, PaaS, IaaS.

INTRODUCTION
Cloud computing is still developing standard and processing is viewed as an interest administration. The storage and analysis are releasing great improve due to the performance of cloud computing and in this era, that money and time-consuming applications are feasible for this enormous resource sharing technology. The users are presently experiencing a key in the information technology world, from in-house generated computing power into utility-supplied computing called cloud computing. In cloud computing resources are delivered over the internet as a web service. Recently, there has been a dramatic increase in the popularity of cloud computing systems that rent computing resources on-demand, the bill on a pay-as-you-go basis, and many users on the same physical infrastructure [1]. The cloud computing environment provides an illusion of infinite computing resources to users. The user can increase or decrease their resource consumption rate according to their demands, like electricity. Users are least bother about how and where it generated from rather just make use of it as per our need. When cloud computing concepts extend to information technology, they are neither concerned where the computing services are delivered nor how it functions internally. The cloud computing itself it is considered to be fully virtualized system that allows data computation, storage, and software resources together and server as a single platform. It offers computing services in an efficient and transparent manner. The computing technologies such as cluster, grid, and cloud all aim at allowing access to a large number of computing resources from a fully virtualized system, by seamlessly aggregating resources and offering a single system view. In addition, cloud technology delivers computing service as utility computing. The utility computing describes a business model for on-demand delivery of computing services. In this model, user pay to service providers based on the consumption of service. In similar to the way, as users obtain traditional public utility services such as water, electricity, gas, and telephony. Clouds have become a part of the competitive market today. Many organizations make use of cloud services. While cloud service is rising and gaining popularity, the fear about the use of cloud services is still an open issue. Various issues deterring adoption are identified in the literature; one of the major ones is security. Security risk in the area of the cloud has attracted attention since its beginning. New protocols and tools are always in demand to enhance the security strength of a cloud computing service or service provider.

A variety of cloud service providers are accessible with their services in the cloud environment. These services come along with various specifications, features, and methods of achieving security. Some services focus on secure access to a service and data by encryption, and some are focusing on the secure network itself. Techniques approved by various providers to achieve security are of varying nature. A cloud user may seek a service based on his requirement and level of security provided by a service. To analyze a particular service based on its various security properties is a challenge. The major challenge is to trust a cloud service or service provider in terms of security. One can attempt to model such confidence in a cloud service, as a kind of trust value. This thesis explores the possibility of building such a framework for trust computation and its various aspects.

RELATED WORK
Cloud computing is a new concept for delivering computing service and largely satisfies emerging requirements of
information technology. It has claimed itself to be of great benefit for users and organizations because it can dramatically reduce the expenses and provide aid to manage information technology systems without any hassle. Due to its large number of advantages, Cloud has been increasingly adopted in many areas, such as banking, e-commerce, retail industry, and academics etc. In addition to its cloud computing also reduces the risk of capital expenditure for IT companies. On the other hand, cloud vendors can deliver more efficient management and coordination of cloud resources to achieve profit optimization and maximization. Subashini and Kavitha [2] suggest that small and medium-size companies can also use cloud computing services for various reasons, as these services provide fast access to their computing resources, applications and reduce infrastructure costs.

Balachandran et al, 2009 [3] discussed the security of SLAs specification and objectives related to data locations, segregation and data recovery. Kresimir et al, 2010 [4] discussed high-level security concerns in the cloud computing model such as data integrity, payment, and privacy of sensitive information. Bernd et al, 2010 [5] discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology related, cloud characteristic, security controls. Subashini et al, [6] discuss the security challenges of the cloud service delivery model, focusing on the SaaS model. Ramgovind et al, 2010 [7] discussed the management of security in cloud computing focusing on Gartner’s list on cloud security issues and the findings from the international data corporation enterprise. Morsy et al, 2010 [8] investigated cloud computing problems from the cloud architecture, cloud offered characteristics, cloud stakeholders and cloud service delivery models respectively. A recent survey by cloud security alliance (CSA) and IEEE [9] indicates that enterprises across sectors are eager to adopt cloud computing but that security is needed to accelerate the cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having a dramatic impact on cloud computing growth. Some studies have been passed out relating to security issues in cloud computing but this work presents a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing operation and service delivery types.

**Characteristics of cloud computing**

Cloud Computing is a type of computing infrastructure that consists of a collection of interconnected computing nodes, servers, and other hardware as well as software services and applications that are dynamically provisioned among competing users. It focuses on delivering reliable, secure, fault-tolerant, sustainable, and scalable services, platforms and infrastructures to the end-users. These systems have goals of providing practically unlimited computing and storage and hiding the complexity of large-scale distributed computing from users. Services are delivered over the Internet or private networks, a combination of these. The cloud services are accessed over these networks based on their availability, performance, capability, and Quality of Service (QoS) requirements.

**Cloud computing models**

They are three basic models introduced by cloud computing SAAS, IAAS, and PAAS. SAAS stands for software as a service, IAAS stands for infrastructure as a service and PAAS stands for the platform as a service [10].

**Software as a service**

SaaS is a facility or service model of cloud which existing an on-request online subscription of software. Similarly with the other cloud service models, “SaaS” offer organizations by chance to decrease private IT support expenses and exchange upkeep obligation to the SaaS supplier. SaaS is a long shot and most generally utilized by cloud transport shows on grounds that basically every product merchant is hoping to put

![Diagram of cloud computing models](https://via.placeholder.com/500)

**Fig 1. NIST definition of cloud computing**

535
its offering on the Saas rails there are Saas offerings in each class of programming items, and it would presumably take days to rundown all Saas programming sellers in this paper [11].

Platform as a service
PaaS is a cloud service model which affords clients with a configurable application stage including a pre-introduced programming stack. PaaS can be seen in the different signal layer above the equipment, working framework, and virtualization stack. The PaaS shows convey remarkable motivation to organizations because it decreases multifaceted nature of foundation and application upkeep and permits focusing on center programming improvement capabilities. As said in the presentation section, the cost of programming improvement in vast associations is normally lower than the cost of programming and foundation support [12]. Clearly, organizations are gradually moved by reformation their application and middleware frameworks with a specific end goal to enhance efficiency and limit related operational costs.

Cloud security issues
Data Breaches
Cloud providers are the attractive goal for the hackers to attack as huge data stored on the clouds. How much severe the attack depends upon the confidentiality of the data which will be exposed. The information exposed may be financial or other will be important the damage will be severe if the exposed information is personal related to health information, trade secrets and intellectual property of a person of an organization. This will produce severe damage. While data breach happened companies will be fine some lawsuits might happen against these companies and criminal charges also. Sever examinations and client warnings can pile on critical expenses. Aberrant impacts, for example, mark harm and loss of business, can affect associations for a considerable length of time. Cloud suppliers usually express security controls to confirm their surroundings; in any case, associations are in charge of ensuring their own information in the cloud. The CSA has suggested associations utilize multifaceted confirmation and encryption to ensure against information ruptures [14].

Network security
Security data will be taken from endeavour in Saas and processes and stored by the Saas providers. To avoid the leakage of the confidential information data all-overs the internet must be secured. Strong network passage encryption will be involved to secure the network for passage.

Data locality
The Consumer uses Saas applications in the Saas environment provided them by the Saas providers and also processing of their data. In this case, users or clients of clouds are unaware of the fact that where their data is getting stored. Data locality
is much sign of the countries laws and policies regarding the locality of data are strict.

Data access
Data on clouds must be available from wherever anytime and from any system. Cloud storages have some issues regarding the access of the data from any device [15]. Information breaks and different sorts of assaults thrive in situations with poor client verification and frail passwords. Take a gander at the genuine assault on Sony that happened only a few years back. They are as yet feeling the budgetary and social impacts of the hack, which to a great extent succeeded on account of administrators utilizing feeble passwords. The cloud is predominantly appealing target as exhibits a concentrated information store containing high-esteem information and brought together client get to. Uses enter administration frameworks in your cloud condition, are sure that the encryption keys can’t without much of a stretch be discovered on the web. Need solid passwords and place teeth in the precondition via consequently turning passwords and different methods for client ID. To wrap things up, utilize multi-figure validation.

System vulnerabilities
System vulnerabilities are usable program bugs in the OS that programmers deliberately use to control or invade a PC framework. By chance, essential IT cleanliness goes far towards caring you from this sort of genuine assault. Because machines exist in your cloud supplier's server farm, be sure that your supplier hones normal weakness examining alongside convenient security fixes and overhauls.

Account hijacking
You may have seen an email that looks true reasonable. You tap on a connection, and soon thereafter sirens blast and threatening lights streak as your antivirus program go to fight. Otherwise, then again you may have been authentically adverse and had no evidence that you were recently the casualty of a phishing assault. At the point when clients choose a powerless secret key, or taps on a connection in a phishing attempt, they are at genuine danger of turning into the channel for genuine risk to information. Cloud-based records are no special case. Foundation Solid two variable validation and computerize solid passwords and watchword cycling to help secure yourself against this sort of digital assault.

Permanent data loss
Any information destruction or loss can be permanent harm to the business. Cloud information is liable to indistinguishable dangers from is on-premise information: unintentional cancellation by clients or staff of providers, natural loss or damage, or psychological militant assault. It is the cloud supplier's requirement to make preparations for a human error and to make strong physical server farms. In any case, it should likewise secure against cloud information misfortune by setting up SLAs that incorporate incessant and obvious reinforcement to remote locales, and encoding records in the event of inadvertent information introduction [16].

Shared technology and shared dangers
Cloud suppliers allow administrations to thousands to a huge number of occupants. Administrations run from cloud reinforcement to whole framework, stage, and applications as an administrator. The supplier ought to plan their engineering for solid separation in multitenant designs: a fruitful assault on one client is sufficiently terrible. A multitenant assault that spreads from one client to thousands disaster. When you take a gander at cloud supplier and multitenant administrations, ensure that they have executed multifaceted validation on all server has and work present day interruption location frameworks.

Hacked interfaces and APIs
APIs and UIs are the backbones of cloud computing connections and integration among clients and distributed computing. Cloud APIs' IP addresses uncover the association between clients and the cloud, so securing APIs from irruption or human mistake is basic to cloud security. Work with your cloud supplier and application merchants to make information streams that don't open APIs to simple assault. Put funds into the application to copy dangers in a live situation, and practice visit entrance testing.

Access to data
Data enterprise should be accessed and seen by administration not users. This access will provide the enhanced security to the data over the cloud. Various cloud applications are capable towards client collaboration, still free programming trials and join openings open cloud administrations to pernicious clients. A few genuine assault sorts can ride in on a download or sign in DoS attacks, email spam, computerized click extortion, and pilfered substance are only a couple of them. Your cloud supplier is in charge of a solid episode reaction Structures to distinguish and remediate this source of assault. IT is in charge of checking the quality of that structure and for observing their own cloud condition for manhandling of resources.

Appropriate cloud model for business
Appropriate cloud model for business will be a private cloud. Private cloud is more costly than public clouds but more secure. As they are costly they are more secure. Private clouds are only used by only one organization and the security level is higher than the public cloud. When businesses have confidential information and financial transactions and business secrets are more security is needed. Therefore private clouds are safer than public clouds.
Encryption of backups

Cloud backups of data should be encrypted or else encryption of data does not have any importance if the backups of data are not encrypted. Any of the hackers can get access to these backups if they are not protected with appropriate encryptions. But the backups are not encrypted then the data is not secure. An untested reinforcement is a futile reinforcement. A decade back up overcomes the security controls in the generation condition. Data should be secured over its whole lifecycle.

Secure data destruction

Secure destruction of data is necessary when needed. But the damage of data is not protected then the risks of data leakage are present. Somebody can recover that data while the data is not destructed safely. During the occasion that you have put away delicate information in the cloud and if the seller does not properly macerate information from the decommissioned device, the information is unnecessarily put at hazard. Get some information about their information annihilation handle.

CONCLUSION AND FUTURE WORK

Cloud computing technology is the emerging technology which provides the facilities of software and hardware over the internet on demand. A less expensive technology to share the resource over the internet. It is a technology that is based on the internet. Despite many advantages, there are lots of issues in cloud computing environment regarding the security of the clouds transactions and data storage over the internet. As cloud users do not know where their data is going to secure and how much it is secured. Be safe to move data on clouds what will be the standards of security to get the services from the cloud providers. In this research, I tried to find out the security issues in the cloud computing environment and which the good architectures for computation are. This research will help the cloud users to understand the security level of cloud computing whether it is safe to migrate to the cloud and what standards must be checked before migrating to clouds. Hence clouds are safe to store data. The proposed scheme showed that better performance when compared with another state of the art scheme for encryption to prevent data breaches. In our future work, we consider other means of preventing data breaches and propose a comprehensive framework that targets all kinds of data breaches.

REFERENCE


