A Study on Challenges and Issues in Cloud Computing

V.Cyril Raj, Ph.D
Professor & Head
Department of CSE/IT
Dr.M.G.R Educational and research institute
University, Chennai.

Justin J Sam
II M.Tech
(Information security & cyber forensics)
Dr.M.G.R Educational and research institute
University, Chennai.

ABSTRACT
Cloud Computing is becoming so popular among organizations and individual users due to its economical and expandable nature. There is a shifting in IT architecture towards cloud computing. The major attractiveness of the technology is its convenience, availability, on-demand network access, scalability, speed etc. Outsourcing data in the cloud relieves the owners of the burden of local data storage and maintenance. Many believe that it will be a revolution in computing after PCs, laptops and smart phones. At the same time, being a technology of infant stage cloud computing faces many challenges and issues. The paper discusses the major challenges and issues of cloud computing.

Keywords

Cloud Computing, Service level agreement (SLA), Denial of Service(DoS)

1. INTRODUCTION
Cloud computing is Internet based computing as the 'cloud symbol' is used to represent the Internet, the computing architecture which is fully based on Internet is so called cloud computing. It provides shared resources, information and applications to other computers and devices on demand which is simply like that of electricity grid. Cloud computing is believed to change potentially the way in which organizations realize their computing and IT needs. IT big bang is happening with enormous potentials for future business environment [1]. By providing an attractive 'pay-per-use' model of computing, it allows organizations to merely focus on their core business while outsourcing their computing and IT requirements is being done by the cloud.Cloud is actually much more than that of traditional server or webhosting, by offering many different layers, components and opportunities. Cloud computing provides an effective solution. It allows the organizations to migrate their data to cloud, which promises high speed access and availability.

2. CLOUD: OVERVIEW
According to the National Institute of Standards and Technology (NIST) [2], Cloud computing can be defined as a model for enabling convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

2.1 Service Models
The cloud computing with current technologies, involved three common models of services as - Infrastructure as a Service (IaaS) which provides a virtualized machine (an environment like a physical machine but with some limitations) to the clients, - Platform as a Service (PaaS) that usually provide an Application Programming Interface (API) to the client so it will be possible to utilize the API and develop customized applications; and Software as a Service (SaaS) with providing an interface (usually web based) to the client for using the intended service [3].

2.2 Deployment Models
There are three deployment models for Cloud computing: public, private, and hybrid [4]-[7].

2.2.1 Public Cloud
The physical infrastructure is generally owned and managed by the service provider.

2.2.2 Private Cloud
The physical infrastructure may be owned by and managed by the organization or the designated service provider [9] with an extension of management and security control planes controlled by the organization.

2.2.3 Hybrid Cloud
This model of Cloud computing is a composition of two or more Clouds (public or private) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability

3. CHALLENGES AND ISSUES
A survey by Gartner shows in the figure below the major challenges that affects the adoption policies for cloud services. The figure shows that security and privacy tops the list. Some of the major challenges and issues faced by the cloud computing are as follows.

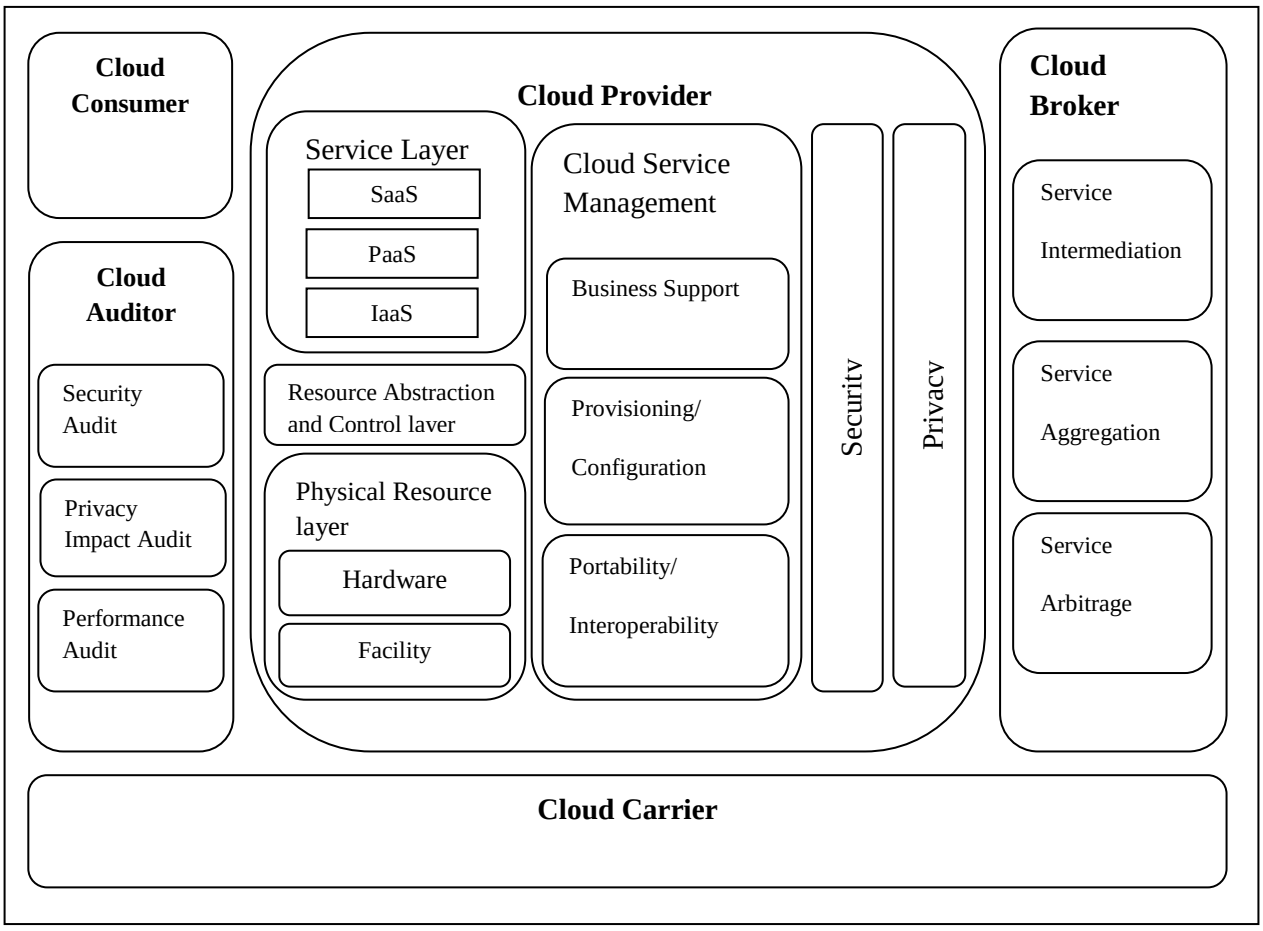

Fig 1. NIST Cloud Reference Architecture.

3.1 Security and Privacy

Security and privacy is always a great concern of the data which is outsourced in the cloud. It is something like keeping some valuables in the locker of a bank which is as safe as until a thief breaks the locker. While considering the confidentiality, integrity and availability of the digital data we can easily say it is more important than just keeping some physical entities. The cloud service provider should not be able to break in to the confidentiality of the data. At the same time checking the integrity is a big issue. Privacy preserving public auditing is a method to ensure the integrity.

3.2 Forensic Challenges for Law Enforcement

Computer forensics is being active for the last decade and it has been expanded in all its dimensions from the infancy. But by the emergence of cloud computing it faces greatest challenges in dealing with. A recent FBI research indicates that the size of the average digital forensic case is growing at the rate of 35% per year indicates the wild increase in digital crimes Since the huge amount of data and the geographical distribution of data affects the forensic examiners in dealing with the cloud for digital investigations. Mobile devices will be enjoying more in the cloud computing platform as it enables them to access the computing power and resources without being available in the local device. More and more users today are depending on mobile devices because of their cost effectiveness, mobility and simplicity. In a country like India the saturation of mobile phone users is being daily increased. But the problem is the law enforcement does not have sufficient mechanisms to trace back to the culprits as 6 out of 10 crimes committed today will involve the use mobile phones. Huge amount of data in cloud computing in distributed locations still makes the efficient digital investigation a dream. Another factor is the cloud service providers are not considering the forensic readiness as an essential requirement compared to the security and availability of the services. An alternative or revised computer forensic process needs to be developed to meet the needs of cloud computing investigations.

3.3 Resource Sharing

In the traditional computing model the resources from same physical entity are used exclusively by a single organization. By the emergence of cloud computing the organizations and states want to share the same physical storage which is used by their competitors too. This situation will not be accepted by the data owners as their data might possess unknown threats from the rivals. Outsourcing the data along with the competitors will create more head ache. For example, a US based IT industry will not like to store their data in a Chinese server even though for the sake of reduced cost. It would be unwise for a business to execute propriety algorithms as

processes on hosts on which their competitors could also run processes, based on the ability of the operating system to enforce process isolation [8].

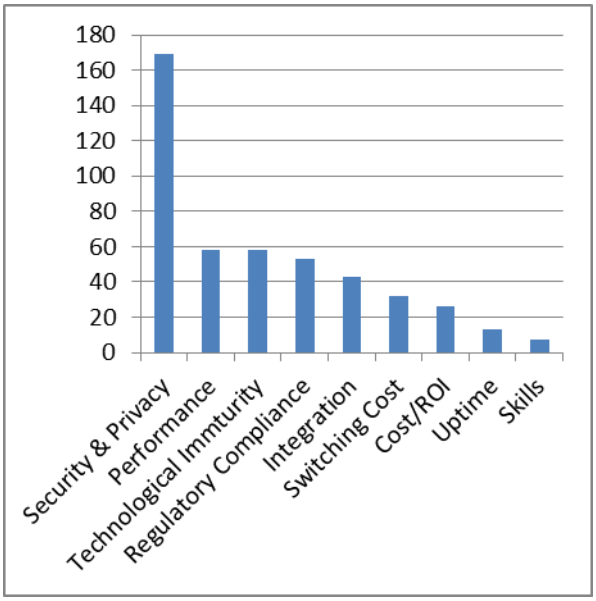

Fig 2. Gartner CIO Survey.

3.4 New Attack Strategies

The intensity and sophistication of attacks against cloud computing resources will increase with the amount of resources outsourced.

3.4.1 Denial of Service (DoS) attacks

Since it is shared of many resources Security analysts believe that cloud architecture is more vulnerable to denial of service attacks. When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power (more virtual machines, more service instances) to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work against the attacker (by providing more computational power), but actually—to some extent—even supports the attacker by enabling him to do most possible damage on a service's availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service [9].

3.4.2 Authentication attacks

Authentication on almost all cloud computing infrastructure is a simple username and password. It is one of the major vulnerability which is faced by the cloud. Secondary form of authentication like site keys, shared secret questions, virtual keyboards, biometrics etc. should be used to make the cloud more difficult to perform the popular attacks.

3.4.3 Cloud Malware Injection Attack

A first considerable attack attempt aims at injecting a malicious service implementation or virtual machine into the Cloud system. Such kind of Cloud malware could serve any particular purpose the adversary is interested in, ranging from eavesdropping via subtle data modifications to full functionality changes or blockings [10].

3.4.4 Side Channel Attacks

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms. Evaluating a cryptographic system's resilience to side-channel attacks is therefore important for secure system design [11].

3.4.5 Unknown sophisticated attacks

Hackers are so patiently working out for finding out the vulnerabilities on the cloud systems since breaking a cloud system will provide major advantages. The method which they are using is still ambiguous. Hackers are always a step ahead of the security specialists. The method to which the attack is being done is always sophisticated which means no one except the attacker does not know about the finding out of loopholes.

3.4.6 Service Level Agreement

Cloud consumers do not have control over the underlying computing resources. Still they have to ensure the availability, reliability and performance of the resources. Consumers have to obtain guarantees form service providers on delivery of service through Service Level Agreements (SLA). SLA represents an understanding between the cloud subscriber and cloud provider about the expected level of service to be delivered and, in the event that the provider fails to deliver the service at the level specified, the compensation is available to the cloud subscriber. This also includes the terms of service cover other important details such as limitation on liability and accountability. This raises a number of implementation problems. For example resource manager want to possess precise and updated information on the resource usage at any particular time with in the cloud. The resource managers need to employ fast and effective decision models and optimization algorithms to do this. It may need to reject certain resource requests when SLAs cannot be met. All these need to be carried out in a nearly automatic fashion due to the promise of "self-service" in the cloud computing. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework [13].

3.5 Choosing what to Migrate

Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). The results clearly specify that organizations have privacy and security concerns. IT Management systems are easy to move to the cloud. The organizations still have a clear image of what all should be migrated to the cloud.

3.6 Legal Issues

Cloud computing exposes the age, formality and complex application of the current laws. Many legal issues are still yet resolved. The legal and regulatory landscape around cloud

computing is by no means static. There are new laws being proposed that could change the responsibilities of both cloud computing tenants and providers. Cloud computing that employs a hybrid, community or public cloud model ‘’creates new dynamics in the relationship between an organization and its information, involving the presence of a third party: the cloud provider. This creates new challenges in understanding how laws apply to a wide variety of information management scenarios’’ [12]

4. CONCLUSION

The paper discussed the challenges and issues of cloud computing. The common cause between all these challenges is mainly the lack of an inclusive global cloud computing standard, which leads to cloud security and privacy issues, absence of a proper cloud deployment framework. An increased understanding of cloud computing and the roles of various stakeholders in this realm is important. Also, legal issues such as jurisdictional issues, cloud stakeholder roles and rights, and technological approaches to solving these problems should be paramount in resource-based cloud computing research and development.

5. REFERENCES

[1] Khalid Rafique, Abdul Wahid Tareen, Muhammad Saeed, Jingzhu Wu, Shahryar Shafique Qureshi, ‘‘Cloud Computing Economics Opportunities And Challenges’’, Proceedings of IEEE IC-BNMT2011

[2] Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, NIST Special Publication, September 2011

[3] Ben Kepes, “Understanding the Cloud Computing Stack SaaS, Paas, IaaS”, Diversity Limited, 2011

[4] R.J. Bayardo, and R. Srikant (2003) Technological Solutions for Protecting Privacy. IEEE Computer, 36(9), p. 115-118.

[5] E. Bertino (2009) Privacy-preserving Digital Identity Management for Cloud Computing. IEEE Data Engineering Bulletin, 32, p. 21-27.

[6] J. Brodkin (2008) Seven Cloud-Computing Security Risks. InfoWorld. seven-cloud-computing-security-risks, p.853.

[7] R. Buyya, C.S. Yeol, and S. Venugopal (2008) ‘‘Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities’’.

[8] Brian Hay, Kara Nance, Matt Bishop ‘‘Storm Clouds Rising: Security Challenges for IaaS Cloud Computing’’ Proceedings of the 44th Hawaii International Conference on System Sciences – 2011

[9] Mohamed H. Sqalli1, Fahd Al-Haidari2 and Khaled Salah3 “EDoS-Shield- A Two- Steps Mitigation Technique against EDoS Attacks in Cloud Computing”, 4th IEEE International Conference on Utility and Cloud Computing, 2011.

[10] Ajey Singh, Dr. Maneesh Shrivastava ‘‘Overview of Attacks on Cloud Computing’’, International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012

[11] Qiasi Luo1, Yunsi Fei2 “Algorithmic Collision Analysis for Evaluating Cryptographic System and Side-Channel Attacks’’

[12] Glen Brunette, Rich Mogull , Cloud Security Alliance ‘‘Security guidance for critical areas of focus in cloud computing’’.

[13] ‘‘Cloud Computing: Issues and Challenges’’ Tharam Dillon Digital Ecosystems and Business Intelligence Institute Curtin University of Technology Perth, Australia University of Technology Perth.

[14] Federal Bureau of Investigation (FBI), “Regional Computer Forensics Laboratory (RCFL)”, Program Annual Report for Fiscal Year 2007, Washington, DC, 2008.