IAAS: Components & Security Issues

Pravina Bhatt [1]
Assistant Professor, Department of Information Technology
Vadodara Institute of Engineering and Technology, Kotambi, Vadodara.
pravina169bhatt@gmail.com, pravina.bhatt@hotmail.com

ABSTRACT

Cloud computing is a vast concept. Today cloud computing is the main area of research for IT professionals. Cloud computing is a widespread lease that encompasses sending hosted services over the Internet. It is paradigm in which the resources that can reduce the rate and complication of service benefactors. This technology promises to reduce operational and capital costs. It is much more than simple internet. It is a concept that allows user to access applications that truly be inherent in at location other than user's own computer system or other Internet-connected devices. There are number of benefits of this construction. As an example new firm masses user tender. This means that they handle cost of servers, they manage software updates that depends service only. Discretion, Truth, Handiness, Legitimacy, and Discretion are necessary for all. Infrastructure as a Service (IaaS) serves as the important layer for the other transport copies, and a deficiency of safekeeping in this level will ultimately disturb the other mockups. This paper elaborates learning of one of such security components namely IaaS and determines susceptibility.

Keywords*: *Computing, Cloud Computing Security, Service Level Agreement (SLA), Infrastructure as a Service (SaaS).

INTRODUCTION

Clouds have large pools of easily usable and accessible virtualized resources. These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing optimum resource utilization. It's a pay-per-use model in which the Infrastructure Provider by means of customized Service Level Agreements (SLAs) offers guarantees typically exploiting a pool of resources. Organizations and individuals can benefit from mass computing and storage centers, provided by large companies with stable and strong cloud architectures. Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software. From one side, cloud computing is nothing new because it uses approaches, concepts, and best usability characteristic that have already been established. From another point of view, everything is new because cloud computing changes how invent, develop, deploy, scale, update, maintain, and pay for applications and the infrastructure on which they run. Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Cloud Computing depends primarily on IaaS layer to pro-vide cheap and pay-as-you-go processing power, data storage, and other shared resources. Cloud computing allows small and medium sized business to outsource their datacenter infrastructure without wasting large expenses on it.

CLOUD COMPUTNG SERVICES

A. *Infrastructure-as-a-Service*

The clients use computing resources such as processing power and storage, and they can also control the environment and the deployment of applications. The Infrastructure as a Service is a provision model in which an organization outsourcers the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Characteristics and components of IaaS include:

1. Utility computing service and billing model.
2. Automation of administrative tasks.
3. Dynamic scaling.
4. Desktop virtualization.
5. Policy-based services.
6. Internet connective

Infrastructure-as-a-Service like Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider's application program interface (API) to start, stop, access and configure their virtual servers, memory and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed it's sometimes referred to as utility computing and as Hardware as a Service (HaaS).

B. Platform-As-A-Service

The platform is typically an application framework, and clients use a hosting environment for their applications. Example Google Application Engine. Platform as a Service (PaaS) is a way to lease hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts.

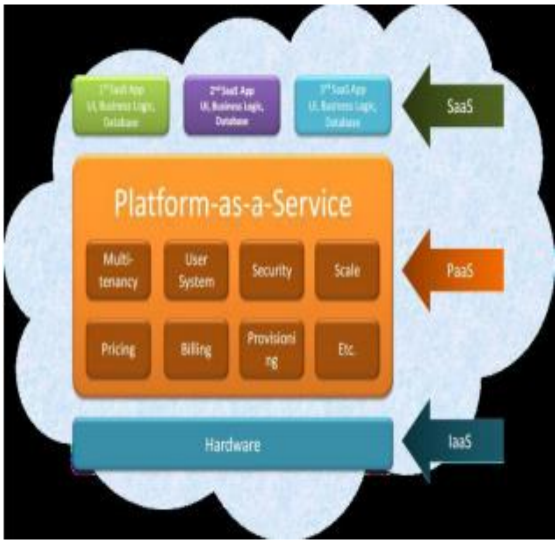

Fig 1: Cloud Computing Services

C. Software-As-A-Service

The clients use applications but cannot control the host environment. Example: Google Apps. Software as a service sometimes referred to as "software on demand," is software that is deployed over the internet and/or is deployed to run behind a firewall on a local area network or personal computer. With SaaS, a provider licenses an application to customers either as a service on demand, through a subscription, in a "pay-as-you-go" model, or at no charge. This approach to application delivery is part of the utility computing model where all of the technology is in the "cloud" accessed over the Internet as a service. SaaS was initially widely deployed for sales force automation and Customer Relationship Management (CRM).

CLOUD COMPUTNG MODELS

A. Public Cloud

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general over the Internet. Public cloud services may be free or offered on a pay-per-usage model. The main benefits of using a public cloud service are:

1. Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider.

2. The term "public cloud" arose to differentiate between the standard model and the private loud, which is a proprietary network or data center that uses cloud computing technologies, such as virtualization. A private cloud is managed by the organization it serves. A third model, the hybrid cloud, is maintained by both internal and external providers. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.

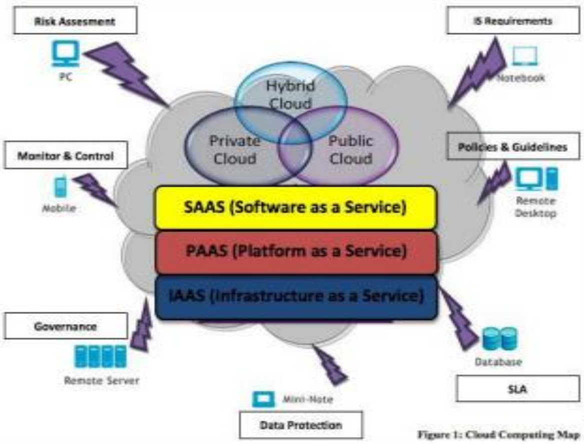

Fig. 2 Cloud Computing Models

B. Community Cloud

A community cloud is a multi-tenant infrastructure that is shared among several organizations from a specific group with common computing concerns. Such concerns might be related to regulatory compliance, such as audit requirements, or may be related to performance requirements, such as hosting applications that require a quick response time. Private cloud (also called internal cloud or corporate cloud) is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall. Advances in virtualization and distributed computing have allowed corporate network and datacenter administrators to effectively become service providers that meet the needs of their "customers" within the corporation. Marketing media that uses the words "private cloud" is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service such as Amazon's Elastic Compute Cloud (EC2). The goal of a community cloud is to have participating organizations realize the benefits of a public cloud -- such as multi-tenancy and a pay-as-you-go billing structure -- but with the added level of privacy, security and policy compliance usually associated with a private cloud.

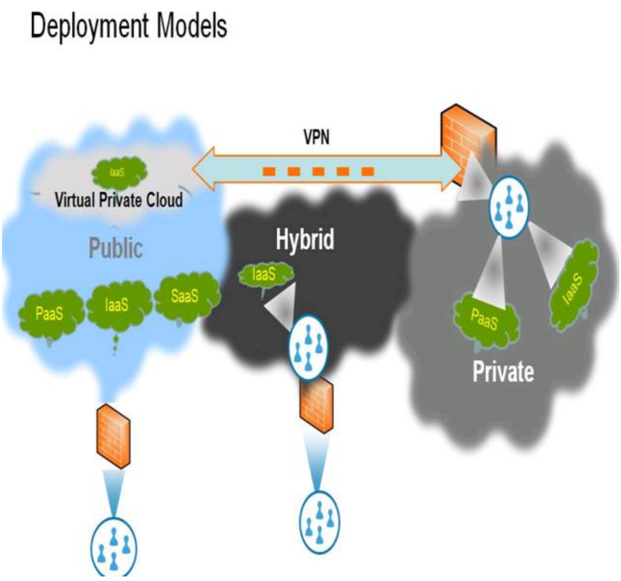

Fig.3 Deployment model of cloud

C. Hybrid Cloud

A hybrid cloud is a Cloud Computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities.

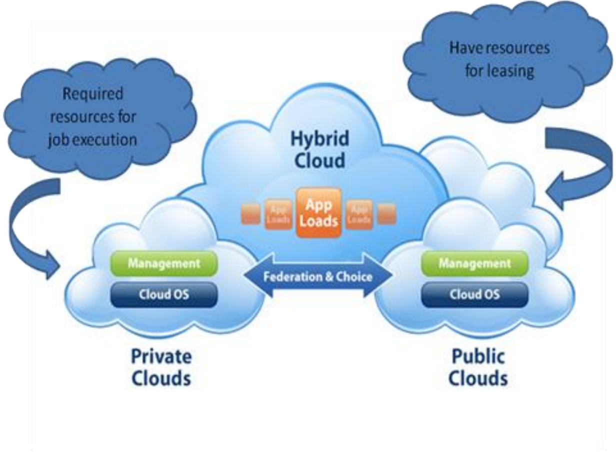

Fig.4 Hybrid cloud

D. Private Cloud

A community cloud may be established where several organizations have same requirements and seek to share infrastructure so as to realize some of the benefits of cloud computing. With the costs spread over fewer users. Private cloud is the phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of public cloud systems.

IAAS COMPONENTS

IaaS delivery model consists of several components. Employing those components together in shared and outsourced environment is primary requirement of IaaS. There are multiple challenges to achieve impede the Cloud Computing adoption. Security and Privacy are the most significant challenges in IaaS. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer will certainly affect the other delivery models. In this section we study the security issue of each component and discuss the proposed solutions and recommendations for them.

A. Service Level Agreement (SLA)

SLA encompasses SLA contract definition, SLA negotiation, SLA monitoring, and SLA enforcement [2]. Using SLA in cloud is the solution to guarantee acceptable level of QoS. SLA contract definition and negotiation stage is important to determine the advantages and duties of each party, any misunderstanding will affect the systems security and leave the client exposure to faults. On the other hand, monitoring and enforcing SLA stage is crucial to build the trust relation between the provider and the client. It is necessary to monitor QoS attributes continuously to enforce SLA in a dynamic environment such Cloud [2]. Web Service Level Agreement (WSLA) framework [3] was developed for SLA monitoring and enforcement in SOA. Using WSLA for managing SLA in Cloud Computing environment was proposed by delegating SLA monitoring and enforcement tasks to a third party to solve the trust problem.

B. Utility Computing

Utility Computing played an essential role in Grid Computing deployment. It packages the resources like computation, bandwidth, storage etc. as metered services and delivers them to the client. There are two main points in this model. First, it reduces the total cost, i.e., instead of owning the resources, client can only pay for usage time. Second, it has been developed to support the scalable systems, i.e., Utility Computing can support grid computing which has the characteristic of very large computations or a sudden peaks in demand which are supported via a large number of computers.. Thus, utility computing shapes two main characteristics of the Cloud Computing. The first challenge to Utility Computing is the complexity of the Cloud Computing. In multiple layers of utility, the systems become more complex and require more management effort from both the higher and the second level providers. For example, the higher provider as Amazon must offer its services as metered services. Those services can be used by second level providers who also provide metered services. Amazon DevPay5, an example for such systems, allows the second level provider to meter the usage of AWS services and bill the users according to the prices determined by the user. The Utility Computing systems can be attractive targets for attackers, so an attacker may aim to access services without paying, or can go further to drive specific company bill to unmanageable levels. The provider is the main responsible to keep the system healthy and well functioning, but the client's practice also affects the system.

C. Cloud Software

There are many open source Cloud software implementations such as Eucalyptus and Nimbus 6; Cloud software joins the cloud components together. Either Cloud software is open source or commercial closed source. We can't ensure the vulnerability and bugs in available software, furthermore, cloud service providers furnish APIs (REST, SOAP, or HTTP with XML/JSON) to perform most management functions, such as access control from a remote location . For example, client can use the Amazon EC2 toolkits, a widely supported interface, to consume the services by implementing own applications or by simply using the web interfaces offered by the provider. In both cases, user uses web services protocols. SOAP is the most supported protocol in web services; many SOAP based security solutions are researched, developed, and implemented. WS-Security, a standard extension for security in SOAP, addresses the security for web services. It defines a SOAP header (Security) that carries the WS-Security extensions and determines how the existing XML security standards like XML Signature and XML Encryption are applied to SOAP messages. Well known attacks on protocols using XML Signature for authentication or integrity protection would be applied to web services consequently affecting the Cloud services. Finally, an extreme scenario is showed the possibility of breaking the security between the browser and the clouds server, and followed by proposal to enhance the current browsers security. Indeed, these attacks belong more to the web services world, but as a technology used in Cloud Computing, web services' security strongly influences the Cloud services' security.

D. Platform Virtualization[3]

Virtualization, a fundamental technology platform for Cloud Computing services, facilitates aggregation of multiple standalone systems into a single hardware platform by virtualizing the computing resources (e.g., network, CPUs, memory, and storage). Hardware level abstraction hides the complexity of managing the physical computing platform and simplifies the computing resources scalability. Hence, virtualization provides multi tenancy and scalability, and these are two noticeable characteristics of Cloud computing As the hypervisor is responsible for VMs isolation, VMs could not be able to directly access others' virtual disks, memory, or applications on the same host. IaaS, a shared environment, demands an accurate configuration of hardware to maintain strong isolation. Cloud service providers undertake a significant effort to secure their systems in order to minimize the threats that result from communication, monitoring, modification, migration, mobility, and DoS. In this section, we discuss virtualization risks and vulnerabilities that affect particularly IaaS delivery model in addition to the recent proposed solutions to guarantee security, privacy, and data integrity for IaaS.

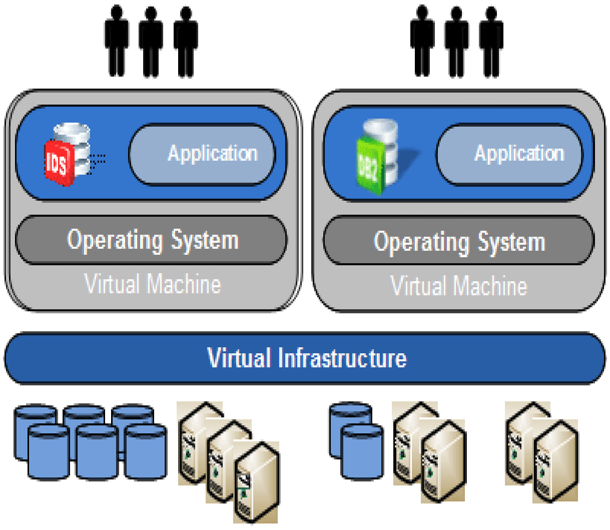

Fig.5 Virtualization model

CONCLUSION

In this paper we discuss about different Layers of Infrastructure as a Service. The SLA's discuss only about the services provided and the l given if the services not met the agreement and the rules, but this waivers don't really help the customers fulfilling their losses. In this Paper we also discuss the Security models and components associated with IaaS. The security issues presented here concern the security of each IaaS component in addition to recent proposed solutions.

REFERENCES

[1] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman,
[2] G. Frankova, Service Level Agreements: Web Services and Security,ser.Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.
[3]L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-Source Cloud-Computing System," Cluster Computing and the Grid, IEEE Interna-tional Symposium on, vol. 0, pp. 124–131, 2009
[4] M. McIntosh and P. Austel, "XML signature element wrapping attacks and countermeasures," Workshop On Secure Web Services, 2005.
[5] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009
[6]P. Patel, A. Ranabahu, and A. Sheth, "Service Level Agreement in Cloud Computing," CloudWorkshops .
[7] R. Kanneganti and P. Chodavarapu, SOA Security. Manning Publications, 2008. [Online].Available: http://www.amazon.com/SOA-Security-Ramarao-Kanneganti/dp/1932394680
[8] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications,p. 9, August 2008. [Online]. Available: http://arxiv.org/abs/0808.3558
[9] SLA Management Team, SLA Management Handbook, 4th ed. Enter-prise Perspective, 2004.
[10] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Se-curity and Privacy: An Enterprise Perspective on Risksand Compliance, 1st ed., 2009