April - June © 2015 Transactions; 2(6): 296-308

International Journal of Research and Applications

ISSN (online): 2349-0020 ISSN (print): 2394-4544 http://www.ijraonline.com/

Survey Report

Survey on cloud computing technologies and security threats

Sumalatha Bandela [1], Ramesh Gadde [2] and Dr. Suresh Pabboju [3]

Corresponding Author:
sumalatha1511@gmail.com

DOI:
http://dx.doi.org/
10.17812/IJRA.2.6(53)2015

Manuscript:
Received: 1st May, 2015
Accepted: 31st May, 2015
Published: 20th June, 2015

Publisher:
Global Science Publishing Group, USA
http://www.globalsciencepg.org/

ABSTRACT

Cloud Computing is one of the emerging technologies in the world. It is a computing technology that provides sharable computing resources like software, platform, storage, applications etc as a service to the customers on demand over the internet. Cloud computing is a Pay-per-Use-On-Demand model that can conveniently access shared IT resources through internet. Its advantages include cost savings, scalability, high availability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. In this paper, we aim to pinpoint the Threats and Security Issues of Cloud computing. This paper first discusses about various cloud based services, use of virtualization in Cloud Computing and then the relation of cloud computing with SOA and Grid computing paradigms. Finally it discusses security threats to cloud computing services.

Keywords: Cloud Computing, Service Oriented Architecture, Virtualization, Grid Computing.

[3] Professor & Head, Dept., of IT, CBIT (Autonomous), Gandipet, Hyd, Telangana, India - 500 075.

[1 2] Research Scholar, Dept., of CSE, Osmania University, Hyd, Telangana, India -500 007.

IJRA - Year of 2015 Transactions:
Month: April - June
Volume – 2, Issue – 6, Page No's:296-308
Subject Stream: Computers

Paper Communication: Through Conference of ICETET-2015

Paper Reference Id: IJRA-2015: 2(6)296-308

DOI: 10.17812/IJRA.2.6(53)2015
eISSN : 2349-0020 & pISSN : 2394-4544

International Journal of Research and Applications (Apr-Jun © 2015 Transactions) 2(6): 296-308
International Conference on Emerging Trends in Electronics & Telecommunications (ICETET-15)

COMPUTERS SURVEY REPORT

Survey on Cloud Computing Technologies and Security threats

Sumalatha Bandela [1], Ramesh Gadde [2] and Dr. Suresh Pabboju [3]

[1 2] Research Scholar, Dept., of CSE, Osmania University, Hyd, Telangana, India -500 007.
[3] Professor & Head, Dept., of IT, CBIT (Autonomous), Gandipet , Hyd, Telangana , India - 500 075.
[1] sumalatha1511@gmail.com, [2] gadde.ramesh@gmail.com, [3] plpsuresh@gmail.com

ABSTRACT

Cloud Computing is one of the emerging technologies in the world. It is a computing technology that provides sharable computing resources like software, platform, storage, applications etc as a service to the customers on demand over the internet. Cloud computing is a Pay-per-Use-On-Demand model that can conveniently access shared IT resources through internet. Its advantages include cost savings, scalability, high availability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. In this paper, we aim to pinpoint the Threats and Security Issues of Cloud computing. This paper first discusses about various cloud based services, use of virtualization in Cloud Computing and then the relation of cloud computing with SOA and Grid computing paradigms. Finally it discusses security threats to cloud computing services.

Keywords: Cloud Computing, Service Oriented Architecture, Virtualization, Grid Computing.

I. INTRODUCTION

Cloud Computing is an internet based computing technology. It is a technology that delivers sharable, dynamically scalable and virtualized resources as a service to the users on-demand over the internet through large data centers. Users consume resources as a service by just paying for what they use. It is a new type of utility computing that provides virtual servers to the users and IT departments on demand. Globalization of computing assets is the biggest contribution the cloud has made to date. The majority of cloud computing infrastructure consists of reliable services delivered through data centers and built on servers with different levels of virtualization technologies. For users, the cloud appears as a single point of access for all their computing needs. Cloud-based services are accessible anywhere in the world as long as internet connection is available.

As with any new technology, the definition of cloud computing is changing with the evolution of technology and its services. No standard definition for cloud computing has yet been agreed upon, In the simplest of terms, cloud computing is basically internet- based computing. The term "cloud" is used as a metaphor for the Internet.

According to Buyya et. al. [1] a cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreement.

According to U.S National Institute of Standards and Technology (NIST), "Cloud computing[2] is defined as a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and delivered with minimal managerial effort or service provider interaction". It follows a simple "pay as you go" model.

Cloud Computing is based on five attributes. They are

Multitenancy: Cloud Computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level. Virtual environments are used in Cloud to achieve multi-tenancy.
Massive scalability: It provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.
Elasticity: Users can rapidly increase and decrease their computing resources as needed, as well as release resources for other uses when they are no longer required.
Pay per use: Users pay for only the resources they actually use and for only the time they require them.
Self-provisioning of resources: Users self-provision resources

The main feature of Cloud Computing is that computation is done in the "cloud".

Benefits of Cloud Computing

- Infrastructure used in cloud computing environment to provide resources is owned and managed by the cloud service provider and need not be purchased by the customer. So infrastructure cost is reduced.
- Since computing resources are shared among multiple users, utilization rates are minimized. It reduces the infrastructure cost and increases the speed of application development.
- It increases computer capacity dynamically.
- Greater availability of increased high speed band width.
- Agility (increased speed of deployment; faster to market)
- Reduced in-house IT staffing (reduced maintenance costs)
- Enables adoption of latest technology
- Encourages standardization
- Reliability is often enhanced as service providers use multiple redundant sites which support business continuity and disaster recovery.

Cloud providers

A Cloud Provider can be a person or entity or an organization responsible for making a service available to cloud consumers.

- Builds the requested Software/Platform/Infrastructure services.
- Owns and manages the infrastructure used in cloud computing environment for provide the services.
- Providing the services at agreed-upon service levels.
- Provides security and privacy for the services.

Fig 1:Key Cloud Providers

Many companies are delivering services from the cloud. Some notable examples are depicted in fig 1:

Google -- Has a private cloud that it uses for delivering many different services to its users, including email access, document applications, text translations, maps, web analytics, and much more.

Microsoft — Has Microsoft SharePoint online service that allows for content and business intelligence tools to be moved into the cloud, and Microsoft currently makes its office applications available in a cloud.

Salesforce.com — runs its application set for its customers in a cloud, and its Force.com and Vmforce.com products provide developers with platforms to build customized cloud services.

II. CLOUD BASED SERVICES

As shown in Fig 2 Cloud services are offered in terms of Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS), and Software-as-a-service (SaaS).

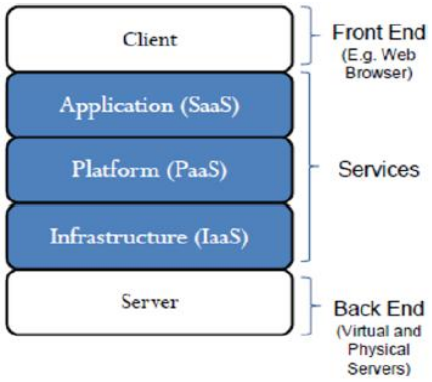

Fig 2: Cloud Service Stack

Software-as-a-Service (SaaS): It is the most widely known and widely used form of cloud computing. It delivers applications to thousands of users via web interface. For a customer, there are no up-front investment costs in server or software licensing. In a SaaS model, the customer does not purchase software, but rather rents it for use on a subscription or pay-per-use model. It is most often implemented to provide business software functionality to enterprise customers at a low cost. SaaS eliminates customer worries about application servers, storage, and application development.

Examples of SaaS providers:

- Salesforce.com is the best know example of SaaS computing which delivers enterprise application via simple website.
- Google Apps provide online access to the most common office and business applications used today via a web browser.
- Yahoo and Google, VoIP from Vonage and Skype etc

Key benefits of a SaaS model

- Applications delivery uses the one-to-many delivery approach, with the Web as the infrastructure.
- Management of a SaaS application is supported by the vendor from the end user perspective, whereby a SaaS application can be configured using an API, but SaaS applications cannot be completely customized.

The SaaS model is a multitenant architecture model, which means the physical backend hardware infrastructure is shared among many different customers, but logically is unique for each customer.

Platform as a Service (PaaS): It is a variation of SaaS. It delivers development environment as a service to the developers who use it to develop, test, deploy, host and manage custom web based applications. PaaS solutions are used for in-house (proprietary) development or for special software or applications on that platform. With PaaS, developers can often build web applications without installing any tools on their computer, and can then deploy those applications without any specialized system administration skills.

Examples of PaaS providers:

- Google App Engine makes it easy to build an application that runs reliably, even under heavy load and with large amounts of data.
- Microsoft's Azure
- Salesforce's.com,
- ADP Payroll processing, US Postal Service offerings etc

Key benefits of a PaaS model

- No maintenance in setting up and running platform and its tools
- Development by (geographically distributed) teams possible

Infrastructure as a Service (IaaS): It delivers computer infrastructure consisting of computer servers, storage, and networking hardware etc are delivered as a service. This infrastructure hardware is often virtualized, so virtualization, management and operating system software are also part of IaaS as well. It allows users to access the underlying infrastructure through the use of virtual machines. Users acquire computing resources such as hardware, processing power, memory and data storage, network bandwidth from an IaaS provider and use the resources to deploy and run their applications

Examples of IaaS service providers include

- Amazon Elastic Compute Cloud (EC2)
- Amazon Simple Storage Service (S3).
- Eucalyptus
- Open Nebula
- Nimbus

Key benefits of an IaaS model

- No maintenance for setting up and running the infrastructure
- Redundant data storage

III. CLOUD DEPLOYMENT MODELS

Cloud Computing model has three main deployment models which are depicted in Fig 3:

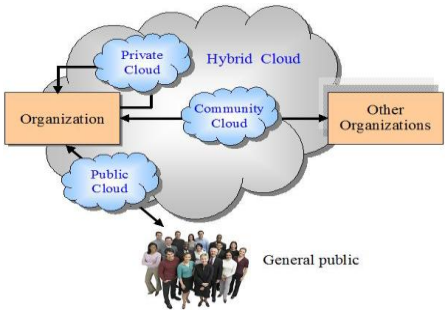

Fig 3: Cloud Deployment Models

Private Cloud: Private cloud refers to a highly virtualized cloud data center located inside the company's firewall. This model is suitable for transmitting classified information like Confidential, Proprietary or Personal information. It is used for critical performance requirements with high availability. The cloud infrastructure is operated solely within a single organization, and managed by the organization or a third party regardless whether it is located premise or off premise. The motivation to setup a private cloud within an organization has several aspects.

- To maximize and optimize the utilization of existing in-house resources.
- Security concerns including data privacy and trust also make also make private cloud an option for many firms.
- Data transfer cost from local IT infrastructure to a Public Cloud is still rather considerable.
- **O**rganizations always require full control over mission-critical activities that reside behind their firewalls. .
- Academics often build private cloud for research and teaching purposes.

Public Cloud: Public Cloud makes the resources, such as applications and storage, available to the general public over the Internet on pay-per-use or free. It offers wide range of capabilities at reduced cost. Many popular cloud services are public clouds including Amazon EC2, S3, and Google App. Engine.

Community Cloud: It shares infrastructure between several organizations from a specific community with common concerns such as security, compliance, jurisdiction, etc. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

Hybrid Cloud: It is a composition of two or more clouds (private, community, or public)

offering the benefits of multiple deployment models. It is a multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one deployment system to another.

TABLE 1 : COMPARISION OF CLOUD DEPLOYMENT MODELS

Feature	Private cloud	Public cloud	Community cloud
Cost effectiveness	High costs due to single ownership	Low costs due to multi-tenancy	Moderate cost savings
Examples	e-Bay	Google.com, Windows azure, Amazon.com, Microsoft	Oracle
Applications	Large Business units	Small Business units, Academic & Govt. Organizations	Health and financial institutions
Infrastructure located at	On /Off premises	Off premises	On / Off premises
Infrastructure owned by	Organization/Third party provider	Third party provider	Organizations/Third party provider
Infrastructure managed and maintained by	Organization/Third party	Third party provider	Organization/Third party
Infrastructure accessible and consumed by	Trusted	Un trusted	Trusted
Regulatory authority	Organization	Service Provider	Community
Security risks	Low risk	High risk	Moderate risk
Organizations Control over security architecture	More	Less	Moderate
Nature of sensitivity of data	Can store and process high sensitive data	Less confidential data	Community Data

IV. SERVICE ORIENTED ARCHITECTURE (SOA) AND CLOUD COMPUTING

Service Oriented Architecture (SOA) [4, 17] is a technology architecture which focuses on building systems based-on services.

A) Definition:

SOA **i**s a design pattern which is composed of loosely coupled, discoverable, reusable, inter-operable platform agnostic services in which each of these services follow a well defined standard. Each of these services can be bound or unbound at any time and as needed.

A Service Oriented Architecture (SOA) is intended to define

- Loosely coupled and interoperable services/applications
- A process for integrating these interoperable components.

A service is a function that is well defined, self-contained, and does not depend on the context or state of other services. Services generally communicate using standard protocols, which allows for broad interoperability. New services can be added or created without effecting existing services. In essence, SOA adds the agility aspect to architecture, allowing us to deal with system changes using a configuration layer rather than constantly having to redevelop these systems.

B) Primary benefits of an SOA

- Reuse of services and behaviors. In other words, SOA enables use of the same application functionality (behavior) over and over again without having to port the code, leveraging remote application behavior as if it existed locally.
- The ability to change business processes on top of existing services and information flows, quickly and as needed, to support a changing business.
- Monitoring points of information and points of service, in real time, to determine the well-being of an enterprise or trading community. Moreover, SOA provides the ability to change and adjust processes for the benefit of the organization in real time.
- The ability to expose certain enterprise processes to other external entities for the purpose of inter-enterprise collaboration or shared processes.

C) Relation between SOA and Cloud Computing

SOA can be used as a key technology-enabling approach to leverage cloud computing. As part of enterprise architecture, SOA provides the framework for using cloud computing services. Cloud architecture attached to grid computing ensure that the SOA applications take advantage of the elasticity of the cloud (and also grid computing) to process a service within a finite amount of time. The true success of SOA application depends widely on its deployment in the cloud and taking advantage of its elasticity.

Cloud computing and SOA are different concepts, but they are related. SOA is a pattern of architecture, whereas cloud computing is an instance of architecture, or an architectural option. SOA is more holistic and strategic, meaning it deals with the complete enterprise including the business drivers, whereas cloud computing is more tactical and is a way of solving a problem.

V. VIRTUALIZATION IN CLOUD COMPUTING

Virtualization is the technology that hides the physical characteristics of a computing platform from the users, instead presenting an abstract, emulated computing platform [16]. This emulated computing platform for all practical purposes behaves like an independent system, but unlike a physical system, can be configured on demand, and maintained and replicated very easily. The computing infrastructure is much better utilized, leading to lower upfront and operational costs.

IT organizations have increasingly used virtualization technologies to create a different kind of separation.

A) Definition

Virtualization refers to the logical creation of an IT resource that doesn't physically exist.

It is a method of running multiple independent virtual operating systems on a single physical computer.

Examples of virtualization include the creation of virtual application servers and virtual storage devices like hard drives etc.

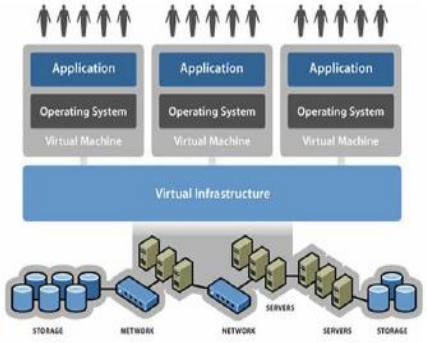

Fig 4: Virtualization Mechanism

B) Different types of Virtualization

There are many different types of virtualization, including hardware, software, desktop, memory, storage, data and network virtualization. Hardware virtualization is one of the most common types of virtualization.

- Platform virtualization refers to creation and management of virtual machines. It is the logical partitioning of physical computing resources into multiple execution environments, including servers, applications, and operating systems. Virtualization is based on the concept of a virtual machine running on a physical computing platform. Virtualization is controlled by a Virtual Machine Monitor (VMM), known as a hypervisor. Xen, an open-source hypervisor, is widely used for cloud computing.
- Desktop virtualization is also another widely used type of virtualization that creates and stores a client's desktop on a server that can be remotely accessed by the client over a network.
- Software virtualization allows different versions of an operating system to coexist and run on the same physical machine, providing the ability to run applications in different environments without the need to invest in additional hardware.

C) Reasons for Companies to move into Virtualization

Reason	Benefit
Server Consolidation	Savings in hardware, environmental costs, management, and administration.
Legacy Applications	Ability to run legacy applications that will not run on newer hardware and/or OS.
Build Secure Computing Platforms	Provides secure, isolated sandboxes to run un trusted applications.
Create Operating Systems	Resource limits and guarantees
Simulate hardware and hardware configuration	The illusion of running multiple processors and to simulate networks of independent computers.
Task Management	System migration, backup, and recovery

D) Advantages

Some of the key benefits of virtualization [15] that are indigenous to cloud computing are as follows:

- Security is provided by compartmentalizing environments with different security requirements in different virtual machines and one can select the guest operating system and tools that are more appropriate for each environment. A security attack on one virtual machine does not compromise the others because of their isolation
- reduction in energy consumption
- Provides cost reductions by consolidation smaller servers into more powerful servers. Cost reductions stem from hardware cost reductions, operations cost reductions in terms of personnel, floor space, and software licenses etc.
- Maximizes return on investment for the computer
- Facilitates the smarter and more efficient use of IT resources within an enterprise

- Billing based on usage (utility pricing) and not fixed hardware capacity
- Rapid deployment of additional servers
- Promotion of economies of scale
- Separation of the customer from physical server locations
- Usage based on service-level agreements
- Alternative sourcing supported
- Fault tolerance
- Application mobility among servers and data centers
- Reliability and availability: A software failure in a virtual machine does not affect other virtual machines

The key enabling characteristics of virtualization are low system overhead for optimum performance and integrated management capabilities in order to deploy cloud application components quickly and flawlessly

E) *Relation between Virtualization and Cloud Computing*

Cloud computing relies heavily on virtualization. Virtualization serves as the basis for Cloud computing architecture the services are built on top of a virtualization layers which help the service providers to manage the service and offer standardized platform to the users. Virtualization is in fact another key element of cloud computing, it enables the service provider to offer the homogeneous service simultaneously to all customers, something that cannot be achieved, for example, in grid computing.

F) Some Terms related to Virtualization :

- *Host*: Virtualization platform running hypervisor software.
- *Hypervisor Software*: A central program used to manage virtual machines (guests) within a simulated environment (host).
- *Hypervisor*
  - Primary component of a server virtualization platform.
  - Often referred to as the virtual machine monitor (VMM).
  - Central nervous system within a virtual infrastructure.
  - Manages the host's underlying hardware resources and handles all guest-initiated operating system and application requests for CPU, memory, I/O, and disk resources.
- *Virtual Machine(VM)* : A VM is a group of files that represents a hardware-based computing platform, complete with storage, memory, and configuration components

G) Challenges introduced by Virtualization

1) Tracking of virtual-to-physical mapping & vice versa

Large-scale virtualization by CSPs allows higher resource utilization and adaptation to peaks and troughs in users' demand for computation and storage. However, the addition of virtualized layers also means that accountability requires the identification of events not only on the virtual server, but also the physical server. Currently, there are only tools (e.g. HyTrust []) which are able to log virtual-level logs and system health monitoring tools for Virtual Machines (VMs). There is still a lack of transparency of (1) linkages between virtual and physical servers, (2) relationships between virtual and physical server locations, and (3) how files are written into both virtual and physical memory addresses. Such information is currently not available as a single-point-of-view for the customers.

2) Multiple operating system environments to track

Many different operating systems are available for VMs, and this potentially introduces the need to manage the logging of machines in the cloud which uses a large number of different operating systems. Enforcing a single operating system for all VMs would solve this issue, but it would make the provider less competitive.

VI. GRID COMPUTING AND CLOUD COMPUTING

Grid computing [6] combines computers from multiple administrative domains to reach a common goal, to solve a single task.

A) Definition

Grid computing [7] is a form of distributed computing that involves coordinating and sharing computing, application, data and storage or network resources across dynamic and geographically dispersed organization. In grid computing, servers, storage, and networks are combined to form powerful computing resource nodes that can be dynamically provisioned as needed.

B) Grid Characteristics

Large scale, Geographical distribution, Heterogeneity, Resource sharing, Multiple administrations, Resource coordination, transparent access, Dependable access, Consistent access, Pervasive access.

C) Similarities between Grid and Cloud Computing[8]

- To reduce the cost of computing
- increase reliability,
- increase flexibility by transforming computers from something that we buy and operate our-selves to something that is operated by a third party

D) Differences between Grid and Cloud Computing[9,10,11,14]

TABLE 3 : GRID COMPUTING VS. CLOUD COMPUTING

	Grid Computing	**Cloud Computing**
Means of utilization	Allocation of multiple servers onto a single task or job	Virtualization of servers; one server to compute several tasks concurrently
Typical usage pattern	Typically used for job execution, i.e. the execution of a program for a limited time	More frequently used to support long-running services
Level of abstraction	Expose high level of detail	Provide higher-level abstractions
Task Size	Single Large	Small and medium
ComputationService	Maximum computing	On-demand
Accessibility	Offers dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities.	Offers customized, scalable and QoS guaranteed computing environments for users with an easy and pervasive access.
Infrastructure	A decentralized system, which spans across geographically distributed sites and lack central control. It normally contains heterogeneous resources, such as hardware/software configurations, access interfaces and management policies.	A central computer server with single access point and spans several computing centers, like Google and Amazon, in general contain homogeneous resources, Operated under central control.
Middleware	Full-fledged middleware with well-defined industry standards	still underdeveloped and lacks of standard
Virtualization	Virtualization of data and computing resources	Virtualization of hardware and software platforms

VII. SECURITY THREATS

The biggest challenge in cloud computing is Security. Following are the threats in cloud computing [18].

Attack	Description	Counter measure
DOS	Hackers overflow a network server or web server with frequent request of services thus making them unavailable to legitimate client requests. The occurrence of a DoS attack increases bandwidth consumption besides causing congestion, making certain parts of the clouds inaccessible to the users.	1) Reduce the privileges of the user that connected to a server. 2) Using an Intrusion Detection System (IDS) is the most popular method of defense against this type of attacks. Each cloud can be loaded with separate IDS. And different intrusion detection systems work on the basis of information exchange.
Phishing Attack	Hacker attacks by allowing users to access fake web link. It affects the privacy of user's sensitive information that should not be revealed.	By identifying the spam mails.
Wrapper attack	Attacker can duplicate a fragment of XML signature and add additional codes to control the computer to do what he wants to do.	Use the digital certificate e.g. X.509 authorized by third party such as certificate authorities and also uses the mixture of WS-security with XML signature to a particular component.
Man in the Middle Attack	Data communication between two parties could be hacked by the middle party. Ex. attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. Man in the middle attacks is sometimes known as fire brigade attacks.	1) SSL should properly install and it should check before communication with other authorized parties. 2) Set up an intrusion detection system. 3) Implementing dynamic host configuration protocol (DHCP) snooping on switches can limit or prevent ARP spoofing. This in turn can help you prevent man in the middle attacks.
Backdoor Channel Attack	Hacker by comprising valid user's virtual machines provides rights for accessing victim's resources. This attack can affect the service availability and data privacy. It is a Virtual Machine level attack, Hypervisor level attack.	1)Perform better authentication and authorization 2) Provide strong isolation between virtual machines.
Network Sniffing	During communication , unencrypted data are hacked through network like passwords that are not properly encrypted	Use Encryption methods for securing the data.
Port Scanning	Attacker scans for the open ports and sends packets to the machine varying the destination port. It helps in knowing the services being run in your machine and about the OS	Firewall help to secure the data from port attacks.

SQL Injection Attack	SQL Injection is one of the highest possibilities in a SaaS application. It is a method of attack where an attacker can exploit vulnerable code and the type of data an application will accept, and can be exploited in any application parameter that influences a database query like parameters within the URL itself, post data, or cookie values. If successful, SQL Injection can give an attacker access to backend database contents, the ability to remotely execute system commands, or in some circumstances the means to take control of the server hosting the database.	1) SQL Injection arises from an attacker's manipulation of query data to modify query logic. The best method of preventing SQL Injection attacks is thereby to separate the logic of a query from its data. This will prevent commands inserted from user input from being executed. 2) Properly validating user input for both type and format. 3) Use Stored Procedures that require a very specific parameter format, which makes them less susceptible.
Cross Site Scripting	User enters right URL of a website and hacker on the other site redirect the user to its own website and hack its credentials. It can provide the way to buffer overflows, DOS attacks and inserting spiteful software into the web browsers for violation of user's credentials.	1) Most cross-site scripting attacks occur either with error pages or with parameter values. Therefore the product needs to look for cross-site scripting signatures either within parameter values or within requests that return error messages. To look for signatures in parameters values the product must parse the URL correctly and retrieve the value part and then search for the signature on the value while overcoming encoding issues. To look for signatures in pages that return error messages the product needs to know that the specific URL returned an error code 2) To prevent these attacks, dangerous characters must be filtered out from the web application inputs. These should be filtered out both in their ASCII and HEX values. 3) Disabling scripting languages in the Web browser as well as the HTML-enabled e-mail client -- provides the most protection but has the side effect of disabling functionality. 4) By following links from the main Web site for viewing will significantly reduce a user's exposure while still maintaining functionality.

IP Spoofing	IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.	1)Implementing hierarchical or one-time passwords and data 2)Use of encrypted protocols 3) By installation and implementation of firewalls that block outgoing packets with source addresses that differ from the IP address of the user's computer or internal network. 4) Ingress filtering which uses packets to filter the inbound traffic.
Service Injection Attack	Hacker injects malicious service through accessing service identification files and provides this service to users instead of valid service. This attack affects service integrity. It is an Application level attack, Virtual Machine level attack	1)Use secure web browsers and API's 2)Use hash function to check service integrity 3)Provide strong isolation between virtual machines
DNS Poisoning	It is corruption of an Internet server's domain name system table by replacing an Internet address with that of another, rogue address. When a Web user seeks the page with that address, the request is redirected by the rogue entry in the table to a different address. At that point, a worm, spyware, or other malware can be downloaded to the user's computer from the rogue location.	Populate the etc/hosts file with DNS entries of important servers. This file should be updated through a secure procedure.
ARP Poisoning	It is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised.	Use static ARP tables

IX.CONCLUSION

Cloud computing is a combination of several key technologies that have evolved and matured over the years. Cloud computing changes the way in which IT services are delivered. Minimal investment, cost reduction, and rapid deployment are the main factors that drive industries to utilize. This paper discussed the key benefits of various cloud based services, benefits of using virtualization in cloud computing, Service Oriented Architecture (SOA) and its relation with Cloud Computing and key differences between Grid and Cloud Computing. It also discussed threats to cloud computing and suggested solutions.

REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Gener", Computer Systems, 25(6), pp. 599-616, 2009

[2] Peter Mell, Timothy Grance., "The NIST Definition of Cloud Computing", Sep 2011.

[3] F. Sabahi, "Security of Virtualization Level in Cloud Computing," in Proc. 4th Intl. Conf. on Computer Science and Information Technology, Chengdu, China, 2011, pp. 197-201.

[4] Yi Wei and M. Brian Blake, "Service-Oriented Computing and Cloud Computing: Challenges and Opportunities", IEEE Internet Computing, vol. 14, no. 6, pp. 72-75, Nov-Dec. 2010.

[6] K. Krauter, R. Buyya, and M. Maheswaran, "A Taxonomy and Survey of Grid Resource Management Systems for Distributed Computing", Jr.of Software Practice and Experience, 32, (2), pp. 135-164, 200.

[7] M.Chetty and .Buyya,"Weaving Computational Grids: How Analogous Are They with Electrical Grids?" Computing in Science and Engineering (CiSE), 4, pp. 61-71, 2002.

[8]I. Foster's. (2008). http://ianfoster.typepad.com/blog/2008/01/theres-grid-in.html

[9] I. Foster, Y. Zhao, I. Raicu and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared", Proc. IEEE Grid Computing Environments Workshop, pp. 1-10, 2008.

[10] L. M. Vaquero, L. R. Merino, J. Caceres, M Lindner. (2009). "A Break in the Clouds: Towards a Cloud Definition". http://portal.acm.org/citation.cfm?id=1496091.1496100.

[11] Members of EGEE-II. "An egee comparative study: Grids and clouds - evolution or revolution. Technical report, Enabling Grids for E-Science Project, June 2008. Electronic version available at https://edms.cern.ch/document/925013/.

[12] Mark Bowker, Virtualization and Cloud Computing Move the SMB Market Forward, June 2012.

[13] Virtualization Overview, www.vmware.com.

[14] Members of EGEE-II. An egee comparative study: Grids and clouds - evolution or revolution. Technical report, Enabling Grids for science Project, June 2008. Electronic version available at https://edms.cern.ch/document/925013/.

[15] eremy Geelan. Twenty one experts define cloud computing. Virtualization, August 2008. Electronic Magazine, article available at http://virtualization.sys-con.com/node/612375.

[16] M.A. Vouk, Cloud computing issues, research and implementations, Journal of Computing and Information Technology 16 (4) (2008) 235–246.

[17] Michael Bell, "Introduction to Service-oriented Modeling", Service-oriented modeling: Service Analysis, Design, and Architecture. Wiley & Sons, 3. ISBN 978-0-470-14111-3, 2008.

[18] "Top Threats to Cloud Computing V1.0", Cloud Security Alliance, March 2010. http://www.cloudsecurityalliance.org/.

[19] "Detecting Service Violations and DoS Attacks". Ahsan Habib, Mohamed M. Hefeeda, and BharatK.Bhargava. http://www.isoc.org/conferences/ndss/03/papers/12.pdf.