Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Emerging Security Issues in Cloud Computing

Abhishek Kumar Srivastav, Irman Ali
M.S in Cyber law and Information Security
Indian Institute of Information Technology, Allahabad, India

***Abstract:** Now a day's everybody ask about cloud computing. Cloud technology is an emerging technology and many organization uses this technology for operating many crucial work Here we are investigating the cloud security management service. Cloud gives relevant facility to access the storage on network from anywhere with variety of security. In this paper we discuss about security issues, their solution and draw some statistics for measurement of growing phase of security incident. Here it is discuss that security need everywhere which is either your local network or private and public cloud.*

***Keyword:** Cloud computing, service model, deployment model, network layer security.*

I. Introduction:

When an application and services move on network that is cloud. Cloud computing was coined for what happens when applications and services are moved into the internet cloud. Cloud computing is not something that suddenly appeared overnight; in some form it may trace back to a time when computer systems remotely time-shared computing resources and applications. At this time many company delivery service over cloud that is follows:

- Microsoft,
- Drop box
- Google
- Yahoo,
- Dropmymail etc.

The following section describes characteristics, benefits, challenges of cloud environment.

II. Characteristics:

Cloud computing have following variety of characteristics:

1-Shared Infrastructure: cloud computing used the virtual software which is enable the sharing of physical resources, storage and networking capabilities. The cloud infrastructure seeks to make the most of the available infrastructure across of multiple user.

2-Broad Network Access: Access of internet in broad range cloud play important roll. It is use standard API for accessing the broad range of devices like as PCs, laptop and mobile devices. Deployments of services in the cloud include everything from using business applications to the latest application on the newest smartphones.

3-Scalability via Dynamic Provisioning: Allows for the provision of services based on current demand requirements. This is done automatically using software automation, enabling the expansion and contraction of service capability, as needed. This dynamic scaling needs to be done while maintaining high levels of reliability and security.

4-Resource Polling: the cloud enables the person to enter and use data within the business management software hosted in cloud network from any place and at any time.

5-Measured Service: going back to affordable and their nature of the cloud computing you have to pay only what you use. You can measure storage, performance, processing bandwidth and number of account.

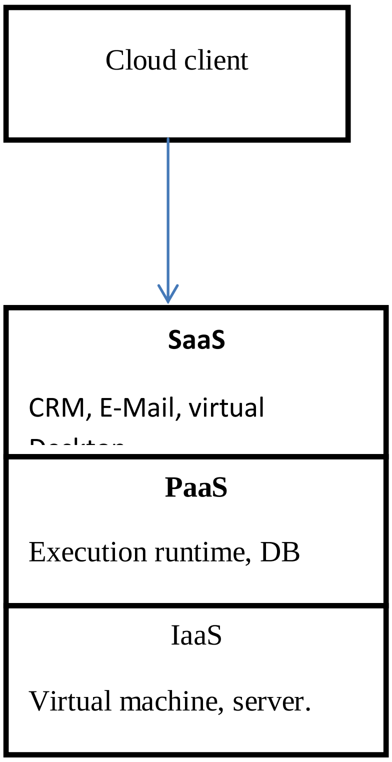
III. Service Model:

Once cloud is established, how cloud computing services & application deploy in terms of business model. The primary model for deployment of cloud services are as follows:

Software as a Service (SaaS): In the service model using software as a service (SaaS), users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. SaaS providers generally price applications using a subscription fee. IN the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud user's own computers, which simplifies maintenance and support. Cloud applications are different from other applications in their scalability—which can be achieved by cloning tasks onto multiple virtual machines at run-time to meet changing work demand. Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user, who sees only a single access point. To accommodate a large number of cloud users, cloud applications can be *multitenant*, that is, any machine serves more than one cloud user organization. It is common to refer to special types of cloud-based application software with a similar naming convention: desktop as a service, business process as a service, test environment as a service, communication as a service.[2]

Platform as a Service (PaaS): In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers like Windows Azure, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually. The latter has also been proposed by an architecture aiming to facilitate real-time in cloud environments.[2]

Infrastructure as a Service (IaaS): In the most basic cloud-service model, providers of IaaS offer computers – physical or (more often) virtual machines – and other resources. (A hypervisor, such as Hyper-V or Xen or KVM or VMware ESX/ESXi, runs the virtual machines as guests. Pools of hypervisors within the cloud operational support-system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements.) IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks(VLANs), and software bundles.[IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks) .To deploys their applications, cloud users install operating-system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis: cost reflects the amount of resources allocated and consumed.[2]

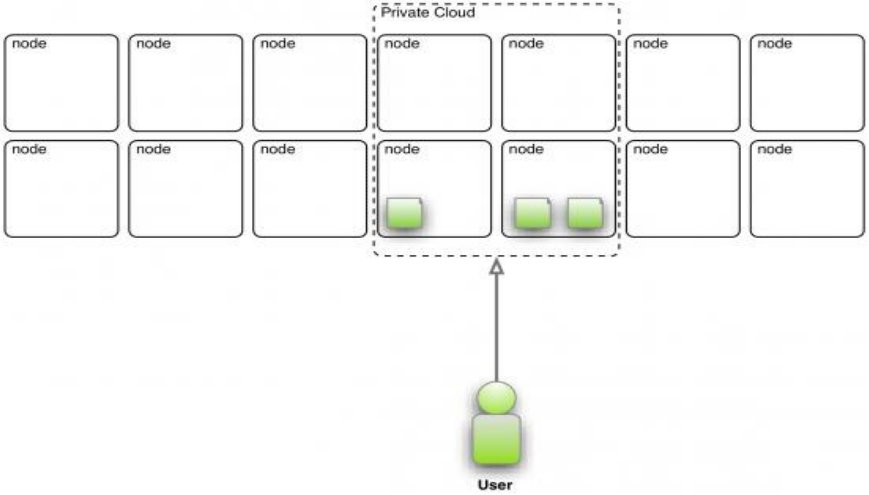


IV. Deployment Model:

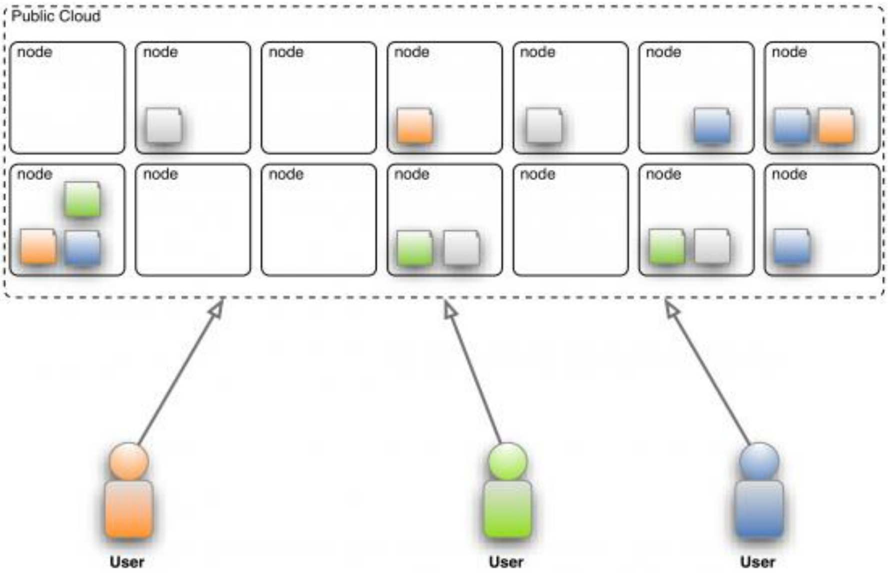
According to service and infrastructure cloud computing can be deploy using following model:

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud.

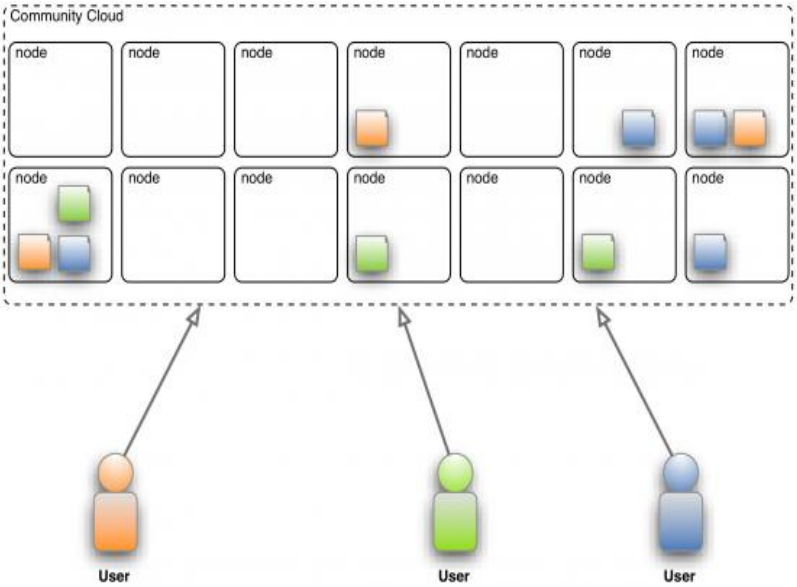
Private Model: The cloud infrastructure maintains and deploy at a specific organization. The operate may be in house or third party.



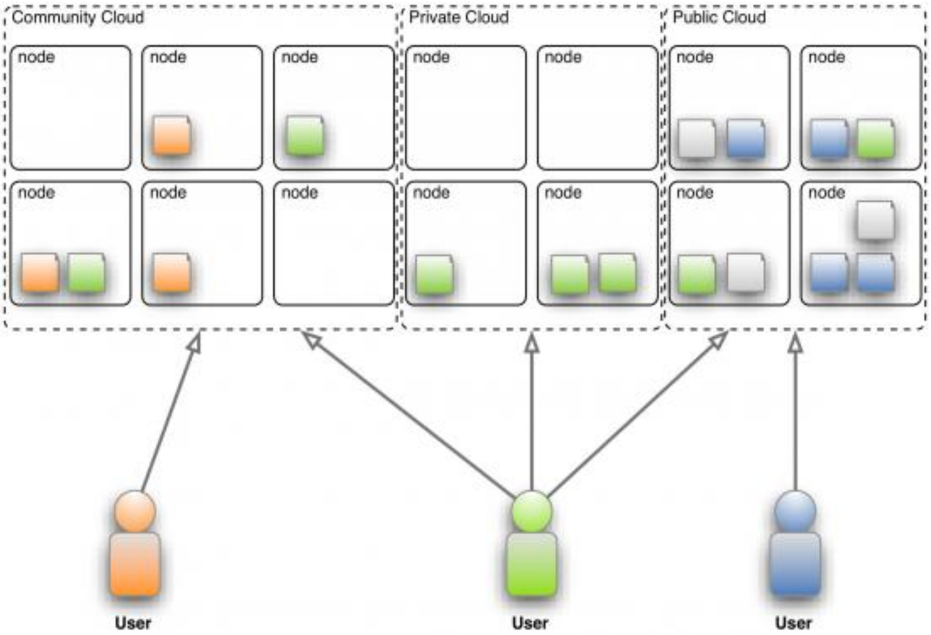
Public Cloud: the deployment of public cloud computing system can be characterize by the public availability of cloud services and application and on other hand by the public network that is used to communicate with the cloud service. The cloud services, application and resources are procured from large number of resources that are shared by all end user.



Community Cloud: A community cloud is multi-tenant in which infrastructure is shared to several organizations from specific group with common computing concern.



Hybrid Cloud: The cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the requirement to retain some data in an organization, and also the need to offer services in the cloud.[1]



Cloud security Issues: according to threat the classification of cloud security are as follows:

V. Basic Security:

Security in different level is necessary in order to implement the cloud computing like as server accessing security, database security, data privacy security. At web application layer the security threat are follows:

Cross Site Scripting*:* In which inject the malicious script into the various web application on internet to exploit the vulnerability. This is mainly two types of method to inject the malicious code : Stored and Reflected XSS. In stored XSS , the malicious code permanently stored into a resource. But in case of Reflected XSS, the malicious code is not stored permanently.

SQL injection Attack*:* In this malicious code injected in the form of sql statement and query. Thus the attacker gains the unauthorized access to database and its content.

Man In Middle Attack*:* In this type of attack an entries try to intrude in middle between client and a sender to inject the false information. The following tools used like: Ettercap, Dsniff etc.

VI. Network Layer Security:

Network basically categorized based on area, distribution and infrastructure. When considering the network layer of security , it is important to distinguish between deployment model of cloud computing. The network layer security basically define as follows:

1-DNS Attack*s:* Domain name server attack on domain server. This is discovered by the researcher Dan Kaminski. DNS attack like as DNS poisoning .Domain Name system Security Extension is responsible to mitigate and remove this type of attack.

2-Sniffer Attack*:* it is occurred when packet transfer from sender to receiver. A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.

3-IP address Spoofing: Most networks and operating systems use the IP address of a computer used to identify a valid and authorized entity. In certain cases, it may be possible for an IP address to be false assumed— identity spoofing. An attacker also use special and malicious programs to construct IP packets that appear to source from valid addresses inside the organization intranet.[1]

After gaining access to the network with a authorized IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.[1]

VII. Application Level Security:

Application level security refers to the use of hardware and software resources to provide application security such that attacker is not able to control over these application.

The following security attacks involve on this level:

1-Denial of Service Attack*:* Denial of Service attack prevents the normal use of computer and network by authorized user.

After gaining access to your network, the attacker can do any of the following:

- Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

2-Dictionary Attack*:* In this attack attacker makes a file with some group of words which is probable by the user to set the password.

3-Buffer Overflow Attack*:* A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

4-Cookie Hijacking*:* In particular, it is used to refer to the theft of a cookie used to authenticate the users to a remote server. It have particular concord to web developers, as the HTTP/HTTPs cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

Statistics for security issues:

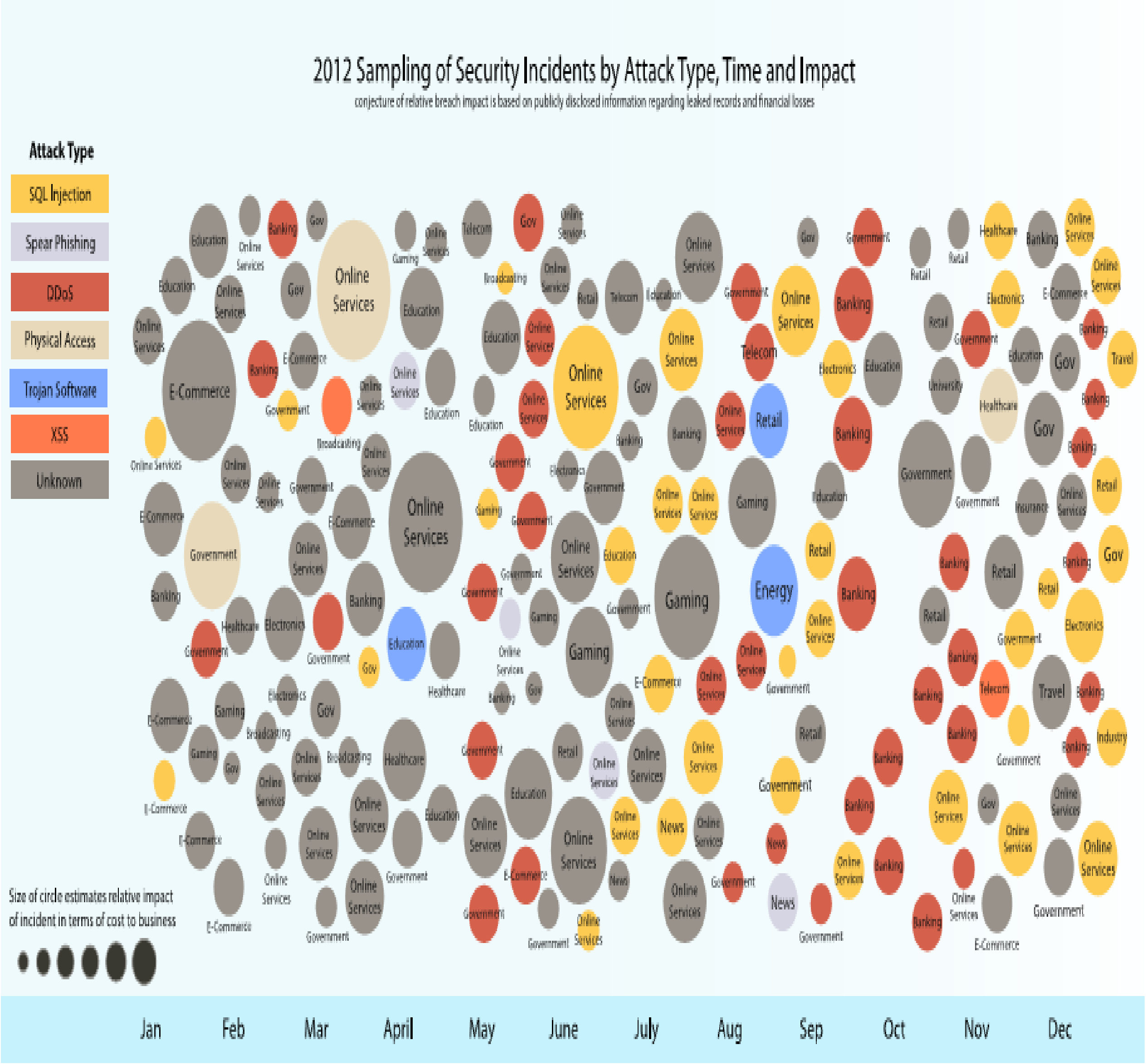


Figure: Attack type

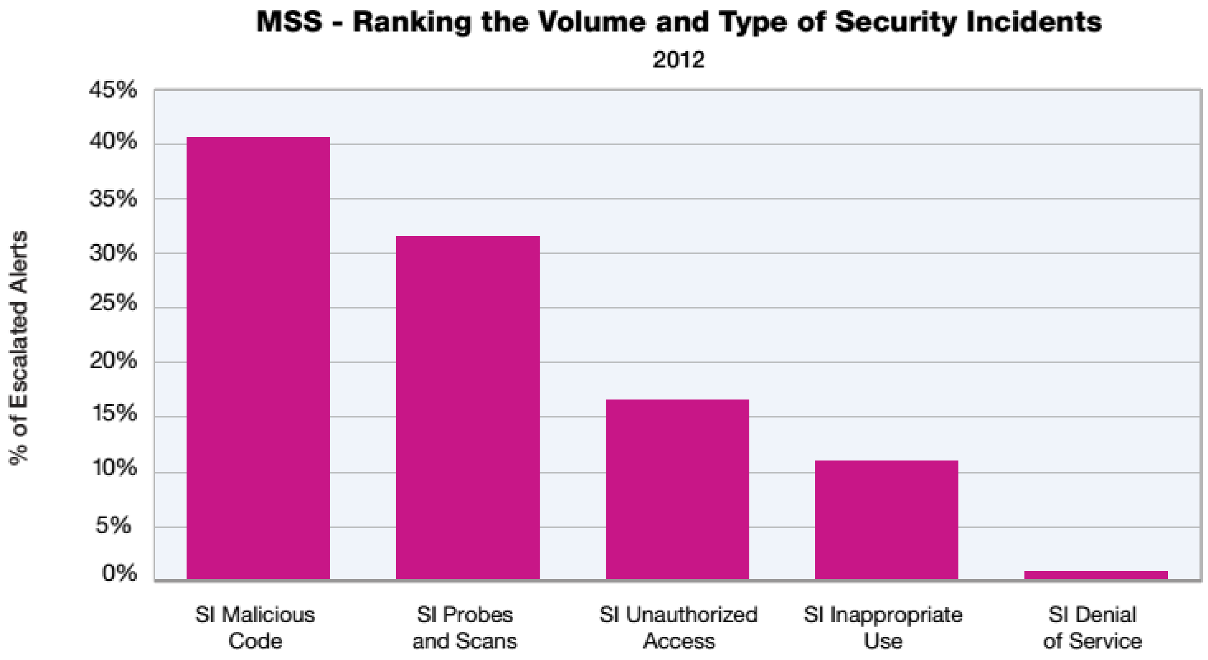


Figure: Ranking of security threat

VIII. Better Solution for Security Issues:

cloud gives better scheme to access the storage on network but there are some security issues, Some solution comes to improve the security issues.

1-Data Encryption Over network*:* developer has to develop application to encrypt and decrypt the data by which data will be secure from unauthorized access.

2-Better Infrastructure*:* the architecture of cloud infrastructure should be secure and configure the network security hardware such that Firewall, IDS,IPS, Proxy Server, Router etc.

3-Data Recovery facility*:* if user loss or destroy their data then cloud vendor provide the data recovery facility to recover the data.

IX. Conclusion:

Cloud computing is a combination of some specific technology. Cloud computing has a potential for cost saving. In this paper we are mainly focused on security issues and their solution . in this paper we also describe the key benefit, characteristics of cloud computing. cloud computing has a potential for virtualization of network environment. Although cloud computing has revolutionized the computing world, it is prone to a number of security threats varying from network level threats to application level threats.

References:

1. http://www.invisibleinc.com/learning-center.php?id=80 , data accessed, jan 26, 2014.
2. http://www.atcloudcomputing.com/ , data accessed, jan 26, 2014.