IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 56-61
www.iosrjournals.org

Security Issues in Cloud Computing

Nisha P.K[1], Meera K Chandran[2], Smitha K.S.[3]

[1]*Dept.of Computer Applications,Sree Narayana Gurukulam College of Engineering,MG University, India*
[2]*Dept.of Computer Applications,Sree Narayana Gurukulam College of Engineering,MG University, India*
[3]*Dept.of Computer Applications,Sree Narayana Gurukulam College of Engineering,MG University, India*

Abstract: *Cloud Computing is the delivery on demand of IT resources and applications through the Internet. It allows to access servers, storage, databases and a huge set of application services over the Internet. The technology behind cloud computing is Virtualization. Cloud computing provides dynamic, reliable, and customizable services. The major concern in cloud computing is Security. Still cloud services are useful some people believe that it is not so safe. Cloud vendors try to ensure security at their maximum. This paper discusses major security issues with cloud computing and the existing counter measures to those security challenges in cloud computing.*

Keywords: *Cloud Computing Security, Virtualization, Network Security.*

I. Introduction

Cloud computing is the delivery of hosted resources over the Internet. With cloud computing, IT companies need not make large investments in hardware and spend a lot of time for managing that hardware. Instead, the company can request the right type and size of computing resources they need to operate the IT department. They can access as many resources they need and only pay for what they use. There are three types of resources that can be consumed using cloud: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (Iaas).

The first type of cloud computing service -Software-as-a-service (SaaS)), in which applications are hosted by a vendor or service provider and is available to the customers over a network. The application is managed by the cloud service provider and the customer needs to pay to use it through a web API. For example, Google Docs relies on JAVA Script, which runs in the Web browser.

The second type of cloud service- Platform-as-a-service (**PaaS**) provides hardware and operating system to deploy and manage applications. So the organizations need not worry about resource procurement, capacity planning, software maintenance, patching, or any of the other heavy lifting involved in running their application.

The third and final type of cloud computing Infrastructure-as-a-service (**IaaS)** delivers virtual machine images as a service and the machine can contain the requirements of the developer .So the developer need not to purchase servers, software, data center resources, network equipment, and the expertise to operate them. Customers can buy these resources from the network cloud. The consumer can automatically change the number of virtual machines to accommodate the changes in their requirement. For example, host firewalls.

II. Cloud Deployment Models

There are mainly four **cloud deployment models**, distinguished by ownership, size, and access. The deployment models which have been suggested by the National Institute of Standards and Technology (NIST) are Public Clouds, Community Clouds, Private Clouds, and Hybrid Clouds.

The Public Cloud: The public cloud deployment model provides services and infrastructure to various clients. An example for public cloud is Google. This service can be provided by a vendor on a free of charge basis or on a pay-per-use basis. The business organizations that need to mange load spikes, host SaaS applications, utilize short-term infrastructure for developing and testing applications, and manage applications which are consumed by many users. This model reduces capital expenditure and bring down operational IT costs.

The Private Cloud: In this model hosting is built and maintained for a specific client. The infrastructure needed for hosting can be on a third-party location. When compared to buying building and managing own infrastructure, this model is not cost efficient.

The Hybrid Cloud: This model helps to host secured applications and data on a private cloud and can use shared data and applications on the public cloud. This type of cloud shares workloads between public and private hosting without any difficulties to the users.

The Community Cloud: Community cloud infrastructure is shared by several organizations with the common policy and agreement considerations. This reduces the costs as compared to a private cloud because it is shared by large groups. The government departments needs to access data relating to population, or information related to infrastructure such as hospitals, roads electrical stations can utilize community clouds.

III. Cloud Computing Architecture

Cloud Computing architecture consists of many cloud components. The two main parts in the architecture are Front End and Back End. These two ends connect to each other using Internet. The front end is the client side and back end is the "cloud" system. The front end consists of the client's computer and the application needed to access the cloud computing resources. The back end consists of computers, servers and data storage systems that create the cloud computing services. A central server administers the system, and monitors the traffic and client demands to ensure everything runs smoothly [2]. It uses a set of protocols and special kind of software called middleware.

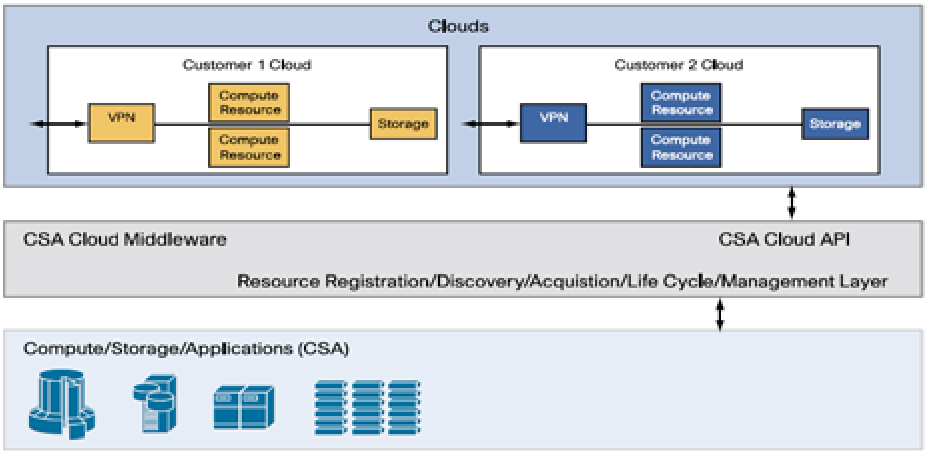

Figure 1. Cloud computing Workflow[3]

A middleware is software that connects computers and devices to other applications. It is the connecting point in client/server. It can be a web server, application server, content management system, or other tool that supports application development and delivery, a software application that connects two or more applications so that data can be shared between them [2]. So it is referred as the cloud OS. Google App Engine and Amazon EC2/S3 are examples of cloud middleware.

Whenever the Client sends service requests, the system management finds correct resources and the client request is executed. Finally, results of the service requests are sent to the clients.

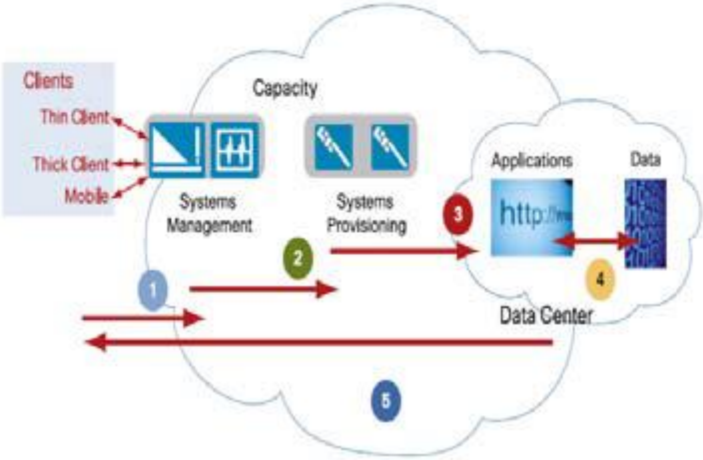

Figure2: Cloud computing Workflow [3]

The next section presents different applications of cloud computing environment and how cloud can be so useful for organizations.

IV. Uses of Cloud Computing.

Practically there are infinite number of applications of cloud computing. Using Iaas, IT companies can save the cost of investing to acquire, manage and maintain the infrastructure. Using PaaS, organizations can increase the speed of development on a ready-to-use platform to deploy applications.

During the period of peak usage of infrastructure, organizations can acquire the additional capacity on a pay-per-use basis from the cloud. Organization does not need to invest huge amount for installing infrequently used infrastructure.

A client can reduce the hardware cost by using a cloud computing system. The client only needs to buy a computer terminal with input devices, a monitor, and just enough processing power to run the middleware needed to connect to the cloud system. The client will find the additional hardware requirements (memory, hard drive) from the cloud.

Complex calculations can take years for individual computer to compute. A client can request a cloud to process a big complex calculation. The cloud will use the processing power of available computers on the back end to speed up the calculation.

Normally organizations have to buy all the needed software or software licenses for every employee for application development. Cloud computing system allows these organizations to access all the required computer applications on a pay-per-use basis.

Social networking platforms provide the basis for analytics on behavioral patterns. Retailers and suppliers can use social networking platforms to extract both structured and unstructured data about the buying patterns of their consumers and can use these data for their marketing campaigns.

The web services interfaces are generally simple. The web applications allow users to store and retrieve their data on a cloud. So at any time and place the data can have high availability, speed, scalability and security.

Cloud computing system will reduce the hardware costs on client side. User will not have to buy the computer with most memory, nor has he to buy the large hard drive to store his data. Cloud system will take care of this client’s need [3]. Client just have to buy a computer terminal with a monitor, input devices with just enough processing power to run the middleware necessary to connect to the cloud system.

Backing up data is a complex and time-consuming operation. Using Cloud-based backup the clients can automatically dispatch data to any location with the assurance that neither security availability nor capacity are issues.

Cloud computing provides considerable advantage over the traditional computing system but it has its own problems. In the next section we discuss about the major security challenges in cloud computing environment and their existing counter measures.

V. Cloud Computing Issues

Before collecting, storing, sharing, processing institutional or personal data in the cloud, the clients should consider significant privacy and security factors. Institutions should conduct careful risk assessment prior to acceptance of any cloud computing service. The security challenges to consider include

V.I **Data Security.**

Getting control over data: When large organizations deploy their applications in the cloud to run, there is a lack of transparency for customers on when, how, and why their data is processed. For example Amazon Simple Storage Service (S3) APIs offer both bucket- and object level access controls. To upload an application the client first creates a bucket in one of the AWS regions. The client can then upload any number of objects in to the bucket using the Amazon S3 API. The bucket names are globally unique, regardless of the AWS region. The clients need to specify the bucket name at the time of creation of the bucket. The client can choose any AWS region that is closer to the client to optimize latency, address regulatory requirements, or minimize costs.

Data integrity: Protecting data from unauthorized deletion, modification or fabrication is referred as Data Integrity**.** Two ways to ensure data integrity are ensuring the integrity of the generating process and ensuring the integrity of input data to the process. Some techniques to ensure integrity of collected data are semantic check, certificate and trusted path .Semantic check is the integration of logic into the process to verify data semantics. Signatures from trusted central authorities is called certificate. Ensuring the data come from an authenticated user or sensing device is the trusted path method.

Risk of subpoena and other government actions: A cloud service provider can store data of different customers. So there is a chance to seize our data by the government because of the illegal actions of some other customers who are hosting in the same server. Our data can be subject to subpoena and other government actions.

Even though the subpoena will compel the cloud provider to turn over user’s data and any access, the data will be secured because we store our data in an encrypted format with a private decryption key, but the provider won’t have user’s access or decryption keys. In this situation, to get a robust service, the cloud service supplier should have more than one data centres and a plan to have them each serve as back up sites to one another in case any one site is hit with an outage**.**

Incompatibility Issue: All clouds are different in nature and in technology. For example Amazon's cloud platform is different from Google's. People expect cross-compatibility between devices, between applications, between platforms and environments. Customers does not care about the incompatibilities inside the working of different cloud services, instead they care about getting data into and out of each cloud and managing functionality within each cloud. To achieve this cloud services should have a common standard.

Regular quality Updating: Cloud vendors frequently adding features, revising old ones, update pricing, trying to stay ahead of the competition and to give incentives to existing customers. The changes in the applications affect both the SDLC (Software development life cycle) and security [3]. Updates to AWS infrastructure are done in such a manner that in the vast majority of cases they do not impact the customer and their Service use[3]**.** AWS communicates with customers, either via email, or through the AWS Service Health Dashboard when there is a chance that their Service use may be affected [3].

cloud server goes out of business: Customers are in fact renting resources like virtual machines, storage space, databases and software’s from the cloud .The resources are available as long as the customers are paying for them, or for as long as the provider stays in business. If the cloud service provider goes down, the customer’s server will go down or their data go along with them. So before selecting a service provider the company must evaluate the risk of the cloud provider,, understand their business model, their long-term plan compatible with the companies' needs etc. Another option to the user is to chose a second provider and use automated, regular backups to make sure any current and historical data can be recovered even if user cloud provider goes down.

V.II Network Security

Security measures are required to protect data throughout their transmission. Data transmission may take place between terminal user and computers.

Distributed Denial of Service Attack: In DDOS attack, servers and networks are busy with a huge amount of network traffic and users are denied the access to some Internet Service. In a worst-case scenario, to perform DDOS attackers use botnets.

Intrusion: In this type of attack, the intruder makes independent connections with the victims and sends messages between them, making them believe that they are talking directly to each other over a private connection; actually the entire conversation is controlled by the intruder.

Spoofing: Internet Protocol (IP) is the widely used protocol for transferring data over the network. Spoofing is the process of creating TCP/IP packets using somebody else's IP address. Attacker gain illegal access to computer, and sends messages to a computer with an IP address indicating that the message is coming from a true host. It is possible for the attacker to redirect the response to his own machine. Amazon EC2 instances cannot send spoofed network traffic. The Amazon's host-based firewall infrastructure will not allow an instance to send traffic with an illegal IP or MAC address.

Port Scanning: While you are in Internet and accessing a server, opens a specific port on the network. A port is a place where information goes into and out of the computer. Port scanning is the process of identifying the opened ports in on a host or on all hosts over a network. Once an intruder has found this information, attacks for destroying these services are tried. It is not possible to stop someone from port scanning our computer because a port will be opened while accessing the internet. In AWS port scanning is a violation of Amazon EC2 Acceptable use Policy (AUP) so these types of violations will consider seriously and it is stopped and blocked.

Packet Sniffing: For most organizations, packet sniffing is usually an internal threat. A third party on the Internet could not easily use packet sniffing software to listen on traffic on a corporate LAN. It is possible for anyone equipped with a laptop can watch communication between machines on a network. Software is used in Packet sniffing, to listen to the raw network device for packets which are interested. When that software sees such a packet, it logs it to a file. It is not possible for a virtual instance to receive or "sniff" traffic that is intended for another instance. Even though, customers can place their interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them .It is not possible for the virtual instances of same customer to listen each other's traffic. Amazon EC2 provides sufficient protection against the customers maliciously attempting to view another's data.

V. III Security Issues

Security issues are very complex in cloud computing because they lie on two tiers: the physical host security and the virtual machine security. If the physical host server's security becomes weak, all of the virtual machines residing on that particular host server are affected. If the virtual machine is weak it affect the working of the physical machine which in create an ill effect on all of the other virtual machines running on that same host [3].

Instance Isolation: Virtualization allows running more than one operating system simultaneously, and also allows running different applications according to the user's demands. Virtual machines running on different organizations are located on the same physical machine on the cloud provider. Physical segregation and Hardware based security does not protect attacks between virtual machines on the same server. A hypervisor isolates different instances running on the same physical machine .This ensures the security of virtual machines from the one which is attacked. If malicious software runs on the server it attacks the hypervisor and access/obstruct other virtual machines.

VI. Standards for Security in Cloud Computing

It is required to have a set of processes, procedures, and practices for implementing a security program. These requirements are collectively known as security standards. These standards in cloud related IT activities include specific steps used to ensure a safe environment in cloud.ie it is used to provide privacy and security of secret information in a cloud environment. Security standards are designed based on a set of key principles planned to protect trusted environment. Defense in depth is a concept that required layers of defense. In this an overlapping system provides security even if one system fails. An example is firewall working in conjunction with intrusion-detection system (IDS) .Because there is no single point of failure and no single entry vector at which an attack can occur, Defense in depth provides security. No single security system is a solution by itself, so it is much better to secure all systems. This type of layered security is developed in cloud computing. Conventionally security was implemented at the endpoints, where the user controlled access. Organization had no choice other than firewalls, IDSs, and antivirus software inside its own network.

Security Assertion Markup Language (SAML): SAML is an XML-based standard data format for communicating authentication and authorization data. The three different roles in SAML specification are: the principal (a user), the service provider (SP) and Identity provider (IdP). The principal asks a service from the service provider. The service provider gets an identity assertion from the identity provider. Based on this assertion, the service provider take an access control decision – in other words service provider can decide whether to perform some service for the connected principal. The IdP may request some information such as a password and user name from the principal before delivering the identity assertion to the SP. Three types of assertions in SAML are between the three parties 1) the messages that assert identity that are passed from the IdP to the SP.2) one identity provider can provide SAML assertions to many service providers. 3) SP may receive assertions from many independent IdPs.

Open Authentication (OAuth): OAuth is a protocol which allows secure API authorization in a standardized and simple method for a variety of web applications. Using OAuth, we can publish and interact with protected data. For developers, OAuth allows users to access their data while protecting account details.

OpenID: It is a decentralized and open standard for access control and user authentication. It helps users to log onto different services using the same digital identity. It is a single-sign-on (SSO) method of access control. Open ID substitutes the regular log-in process, i.e. a password and log-in name, by permitting users to log in once and get access to resources across systems participating.

VI. Conclusion

Cloud computing is a new trend among IT industries because of its lower total cost, extensibility, competitive differentiation, reduced complexity for customers, and faster and reliable services. But still people believe that cloud to be an unsafe place. To gain total acceptance from all potential users cloud computing require some standardization in the security environment and third-party certification to ensure that standards are met.

References

[1]. http://www.leadingedge.uk.net/it-consultancy-services/cloud-computing/what-are-the-types-of-cloud-computing/
[2]. http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm/printable
[3]. https://www.coursehero.com/file/p11mcqr/Clients-will-be-able-to-access-their-applications-and-data-at-any-time-from/
[4]. http://docs.aws.amazon.com/AmazonS3/latest/gsg/AmazonS3Basics.html