ISSN:0975-9646

Navneet Gupta / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1839-1843

Privacy and Security in the Cloud

Navneet Gupta

Assistant Professor, Department of computer Application
Sri Sai University –Palampur H.P.

Abstract-Cloud computing, undoubtedly, has become the buzzword in the IT industry today. It holds the potential to eliminate the requirements for setting up of high-cost computing infrastructure for IT-based solutions and services that the industry uses. It promises to provide a flexible IT architecture, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet from lightweight portable devices.

This would allow multi-fold increase in the capacity and capabilities of the existing and new software. In a cloud computing environment, the entire data resides over a set of networked resources, enabling the data to be accessed through virtual machines. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, Organizations which consider adopting cloud based services must also understand the many major problems of information policy, including issues of privacy, security, reliability, access, and regulation. Cloud Computing leverages many technologies (SOA, virtualization, Web 2.0); it also inherits their security issues.

INTRODUCTION

A new generation of technology is transforming the world of computing. Advances in Internet-based data storage, processing, and services—collectively known as "cloud computing". Many familiar software programs, from email, database storage, games and word processing to spreadsheets, are now available as cloud services. Many of these applications have been offered over the Internet for years, so cloud computing might not feel particularly new to some users.Cloud Computing is a distributed computing model for enabling service-oriented, on-demand network access to rapidly scalable resources.

Such resources include infrastructure as a service (IaaS), development and runtime platforms as a service (PaaS), and software and business applications as a service (SaaS).Cloud computing is one of the most significant transformation in information technology with many advantages to both companies and end users.

The Evolution of Cloud Computing

The increasing popularity of cloud computing is part of an ongoing evolution in how people manage information. Cloud services give organizations of all sizes access to virtually unlimited data storage while freeing them from the need to purchase, maintain, and update their own computer systems. Microsoft and other cloud providers offer "IT as a service," enabling customers to quickly scale up or down as needed and only pay for the computing power and storage they use.

Understanding Risks to Cloud Computing

A major concern with cloud computing is that the cloud provider offers the resources in the cloud, that is, the software, platform and infrastructure to the user (cloud consumer). In addition, user data/information also reside with the cloud The risk with this type of service is that user information could be abused,stolen, unlawfully distributed, compromised or harmed. There is no guarantee that user's information/data could not be sold to its competitor. Unfortunately, this particularrisk applies to all the three types of cloud delivery models, namely, SaaS, PaaS and IaaS. Other risks to cloud computing also exist, and range from privacy, data protection, ownership, location and lack of reliable audit standard to data security procedure of most pioneer cloud providers, such as Google, Amazon, Microsoft etc.

Cloud applications generally fall into one of three categories:

Software as a Service (SaaS):- The cloud provider hosts a single application, such as Hotmail, or a suite of programs such as Microsoft's Office 365. See Fig. 1.0

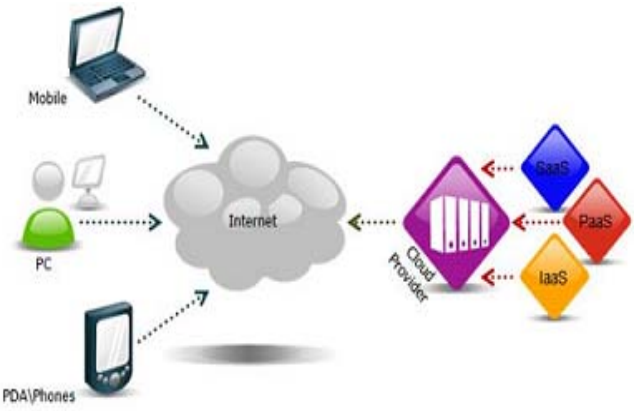

Fig. 1.0 Cloud computing Categories

Platform as a Service (PaaS):-Users create and run their own software applications while relying on the cloud provider for software development tools as well as the underlying infrastructure and operating system. Microsoft's Windows Azur is one such cloud platform.

Infrastructure as a Service (IaaS):- Users rent computing power—either actual hardware or virtualized machines—to deploy and run their own operating systems and software applications.

Similarly, the backend systems that deliver cloud services are generally deployed in one of four ways:

Public cloud. Customers access cloud services and store documents in large datacenters equipped with hundreds of virtualized servers that house data from multiple organizations. See Fig. 2.0

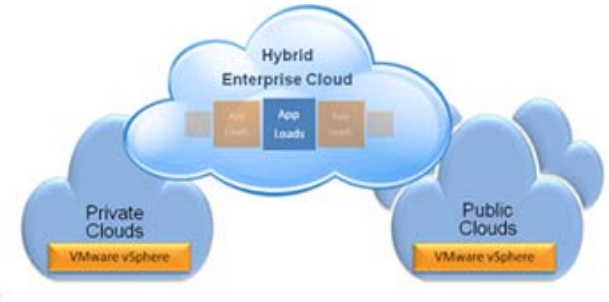

Fig. 2.0 Cloud Services

Private cloud:-A single organization uses a dedicated cloud infrastructure.
Hybrid cloud. Two or more cloud types are linked to enable data and applications to flow between them in a controlled way.

SECURITY ISSUES ASSOCIATED WITH THE CLOUD

There are many security issues associated with cloudcomputing and they can be grouped into any number of dimensions.

There are some specific safety issues
Privileged user access , regulatory compliance, dataLocation, data segregation, recovery, investigative support and long-term viability.

Security issues in a public cloud
In a public cloud, there exist many customers on a shared platform and infrastructure security is provided by the service provider.

The three basic requirements of security:
confidentiality, integrity and availability are required to protect data throughout its lifecycle. Data must be protected during the various stages of creation, sharing, archiving, processing etc. However, situations become more complicated in case of a public cloudwhere we do not have any control over the service provider's security practices.

Multi-tenancy risks: The shared multi-tenant nature of public clouds adds security riskssuch as unauthorized access of data by other tenants using the same hardware. Also, amulti-tenant environment exposes resource contention issues whenever one of thetenants using the hardware consumes a disproportionate amount of resources eitherdue to need or due to hack attacks.

Control and visibility: Businesses have limited control and visibility because the vendoris responsible for completely managing the infrastructure. This adds some additionalsecurity concerns associated with lack of transparency. Business organizations need amental shift as they cede the control of IT to a third party while using public cloudservices.

Security responsibility: Security is a shared responsibility between the vendor and theuser, with the degree of responsibility of each varying by type of cloud model.

Although data is stored outside the confines of the client organization in a public cloud, we cannot deny the possibility of an insider attack originating from service provider's end.

Attacks
As government agencies and businesses migrate to the cloud, they are asking many of the same questions about capabilities of cloud providers. Among them:

1.Cloud-hosted data and applications protected by suitably robust privacy and data management policies? How are the policies enforced?
2. Cloud providers' technical infrastructure, applications, and processes secure?
3. Processes in place to minimize the risk and impact of any incidents that might affect privacy or security?

A. Denial of service (DoS)

Denial of service (DoS) attacks have become a major threat to current computer networks. Attackers could get recognition in the underground community via taking down popular web sites. Because easy-to-use DoS tools, such as Trinoo (Dittrich 1999), can be easily downloaded from the Internet, normal computer users can become DoS attackers as well. They sometime coordinately expressed their views via launching DoS attacks against organizationswhose policies they disagreed with. DoS attacks also appeared in illegal actions. Companies might use DoS attacks to knock off their competitors in the market.
DoS attacks in the Internet generally conquer the target by exhausting its resources, that can be anything related to network computing and service performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles, etc. Recent DoS attacks were launched via a large number of distributed attacking hosts in the Internet. These attacks are called distributed denial of service (DDoS) attacks.
In a DDoS attack, because the aggregation of the attacking traffic can be tremendous compared to the victim's resource, the attack can force the victim to significantly downgrade its service performance or even stop delivering any service.DDoS attacks are more complex and harder to prevent. Since many unwitting hosts are involved in DDoS attacks.
Wireless networks also suffer from DoS attacks because mobile nodes (such as laptops, cellphones, etc.) share the same physical media for transmitting and receiving signals; and mobilecomputing resources (such as bandwidth, CPU and power) are usually more constrained than those available to wired nodes.when a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this: See Fig. 2.1

- The client requests a connection by sending a SYN (synchronize) message to the server.
- The server acknowledges this request by sending SYN-ACK back to the client.
- The client responds with an ACK, and the connection is established.

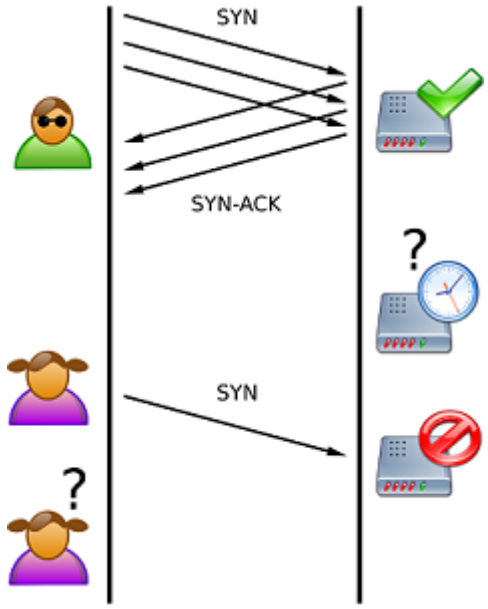

Fig. 2.1 DDos Attack during Establish connection.

The connection between the client and the server is then opened, The abuse arises at the half-open state when the server is waiting for the client's ACK message after sending the SYN-ACK message to the client The server needs to allocate memory for storing the information of the half-open connection. The memory will not be released untileither the server receives the final ACK message. Attacking hosts can easily create half-open connections via spoofing source IPs in SYN messages or ignoring SYN-ACKs. The consequence is that the final ACK message will never be sent to the victim.

There are some tools easily available in Dos Attacks
XML Denial of service also known as X-DoS attack is a content-borne denial-of-service attack whose purpose is to shut down a web service or system running that service. A common X-DoS attack occurs when an XML message is sent with a multitude of digital signatures and a naive parser would look at each signature and use all the CPU cycles, eating up all resources.
Hypertext Transfer Protocol (HTTP) based Denial of Servicealso known as H-DoS in this technique we are using HTTP Flooder &send randomized HTTP requests to the victim web server. With the help of this attack bringing down the cloud system.

B. Smurf Attack
The Smurf Attack is a denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, flooding the victim's computer with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

C. UDP (User Datagram Protocol)
The user datagram protocol (UDP) is a sessionless, or automatic, protocol that sends out packets, or groups of data. Protocols are sets of guidelines, or standards, that manage how data is transmitted over networks such as the Internet. The UDP protocol can be used to initiate a UDP flood attack.

ISSUES IN CLOUD COMPUTING

A. Data Integrity
When a data is on a cloud anyone from any location can access those data's from the cloud. Cloud does not differentiate between a sensitive data from a common data thus enabling anyone to access those sensitive data's. Thus there is a lack of data integrity in cloud computing

B.Data Theft
Most of the cloud Vendors instead of acquiring a server tries to lease a server from other service providers because they are cost affective and flexible for operation.
The customer doesn't know about those things, there is a high possibility that the data can be stolen from the external server by a malicious user.

Physical security
Physical location of data centers; protection of data centers against disaster and intrusion.

A .Data Location
When user use the cloud, user probably won't know exactly where your data is hosted, what country it will be stored in?
Third-party data control
1. .Cloud computing facilitates storage of data at a remote site to maximize resource utilization. As a result, it is critical that this data be protected and only given to authorized individuals.
2. This essentially amounts to secure third party publication of data that is necessary for data outsourcing, as well as external publications.
3. The legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data.
4. All this is prompting some companies to build private clouds to avoid these issues and yet retain some of the advantages of cloud computing.

What is the disaster recovery/business continuity plan ?
While you may not know the physical location of your services, it is physically located somewhere. All physical locations face threats such as storms, natural disasters, and loss of power. In case of any of these events, how will the cloud provider respond, and what guarantee of continued services are they promising?

DATA ISSUES

A. Data Loss :-
Data loss is a very serious problem in Cloud computing. If the vendor closes due to financial or legal problems there will be a loss of data for the customers. The customers

won't be able to access those data's because data is no more available for the customer as the vendor shut down.

B. Data Location :-

When it comes to location of the data nothing is transparent even the customer don't know where his own data's are located. The Vendor does not reveal where all the data's are stored. The Data's won't even be in the same country of the Customer, it might be located anywhere in the world.

PERFOMANCE ISSUES

1. .Application crashes due to poor performance cost money and impact morale. If applications cannot adequately perform during an increase in traffic, businesses lose customers and revenue

2 Sluggish access to data, applications, and Web pages frustratesemployees and customers alike, and some performance problems and bottlenecks can even cause application crashes and data losses.

3 Positive employee productivity relies on solid and reliable application performance to complete work accurately and quickly.

Slow access to applications and data :

Bandwidth is usually the cause, and the most common solution is to add faster network connections.

1. When companies or cloud vendors take the simplistic "more hardware solves the problem" approach to cloud performance, they waste money.
2. Hence, Adding virtual machines may be a short-term solution to the problem, but adding machines is a manual task. If a company experiences a sudden spike in traffic, how quickly will the vendor notice the spike and assign a technician to provision more resources to the account?

ENERGY RELATED ISSUES

1. Cloud computing is rapidly growing in importance as increasing numbers of enterprises and individuals are shifting their workloads to cloud service providers. Services offered by cloud providers such as Amazon, Microsoft, IBM, and Google are implemented on thousands of servers spread across multiple geographically distributed data centers.
2. The electricity costs involved in operating a large cloud infrastructure of multiple data centers can be enormous. In fact, cloud service providers often must pay for the peak power they draw, as well as the energy they consume.
3. Lowering these high operating costs is one of the challenges facing cloud service providers.
4. Moreover, there are other crucial problems that arise from high power consumption. Insufficient or malfunctioning cooling system can lead to overheating of the resources reducing system reliability and devices lifetime.
5. In addition, high power consumption by the infrastructure leads to substantial carbon dioxide (Co2) emissions contributing to the greenhouse effect.

FAULT TOLERANCE

Some techniques are which we will apply

A. Micro reboot techniques
B. Filtering malicious input
C. HA PROXY.

HA PROXY.

1 HA Proxy stands for High Availability Proxy and is used by companies for load balancing and server fail over in the cloud. Companies do not want their website to go down, or worse, for users to notice the site is down.
2. In HA Proxy there is typically a load balancer to distribute the load among a pool of web servers.
3. Whenever a server goes down it is taken out of the pool until it is once again ready to handle requests.
4. HA Proxy has the ability to perform this task by doing periodic health checks on all the servers in a cluster. Even if one of the application servers is not working, users will still have the availability to the application.
5. HA Proxy will properly handle the request from users by redirecting them to the second server, giving the impression that all is well.
6. It monitors all the flow on the network and also health of different servers whenever any server fails it will redirect user request to another server and inform administrator about that faults.

Ensuring security against the various types of attacks

In order to secure cloud against various security threats such as: Smurf Attack, DoS and DDoSattacks, Google Hacking, and Forced Hacking, different cloudservice providers adopt different techniques.

Multi-layer security: In order to ensure data securityand block possible malwares, it consists of multilayersecurity and hence it has a strong securityplatform.

URL filtering: It is being observed that the attacksare launched through various web pages and internetsites and hence filtering of the web-pages ensuresthat no such harmful or threat carrying web pagesare accessible. Also, content from undesirable sitescan be blocked.

Th security model of Amazon Web Services, one of thebiggest cloud service providers in the market makes use ofmulti-factor authentication technique, ensuring enhanced control over AWS account settings and the management of AWS services and resources for which the account issubscribed.In case the customer opts for Multi Factor Authentication (MFA), he has to provide a 6-digit code in addition to their username and password before access is granted to AWS account or services. This single use code can be received on mobile devices every time he tries to login into his/her AWS account. Such a technique is called multi-factor authentication, because two factors are checked before access is granted.

One of the security measures implemented by SalesForce.com& gmail.com to avoid unauthorized access to its platform is sending asecurity code to the registered customer every-time the sameaccount is accessed from same or different IP-address and theuser needs to provide the security code at the time of loggingin, in order to prove his/her identity.

Security issues in a virtualized environment whereinamalicious virtual machine tries to take control of thehypervisor and access the data belonging to other VMs havebeen observed and since traffic passing between VMs doesnot travel out into the rest of the data-centre network it cannotbe seen by regular network based security platforms. Hence, there is a need to ensure that security against thevirtual threats should also be maintained by adopting themethodologies such as: checking the virtual machinesconnected to the host system and constantly monitoring theiractivity, securing the host computers to avoid tampering orfile modification when the virtual machines are off- line,preventing attacks directed towards taking control of the hostsystem or other virtual machines on the network etc.

CONCLUSION :

Cloud computing offers organizations and individuals the promise of enhanced choice, flexibility, and cost savings. To realize such benefits, however, users must have reliable assurances from cloud providers regarding the privacy and security of their personal data. Regulators and lawmakers around the world can help fulfill the potential of cloud computing by resolving legal, jurisdictional, and public policy uncertainties surrounding cloud services.

Cloud computing is technology which enables the user to access resources using front end machines, there is no need to install any software.Every technology has pros and cons cloud computing has also various issues associated with it. . cloud computing provides many services like PaaS(Platform as a service),IaaS(In fracture as a service),SaaS (Software as a service), Daas(Database as a service), HaaS(Hardware as a service).

There are many issues and solutions are highlighted in this topic like security issues, privacy issues, data related issues, energy related issues etc. We are using one of them services like Google docs, Gmail but we do not find such issues related with it. Hence I conclude that this issues comes consider whenever we consider it with big level companies , they are not going to affect much more as single user.

Some of the issues like bandwidth problems will not be longer due to technology are increasing and speed will not affect longer. So there are good scope in this field.

REFERENCES

[1].Tim Mather, SubraKumaraswamy, ShahedLatif,"Cloud Security and Privacy: An Enterprise Edition onRisks and Compliance (Theory in Practice)", O'ReillyMedia, Sep. 2009; ISBN: 978-0596802769.

[2].S. Pearson, "Taking account of privacy whendesigning cloud computing services", CLOUD '09Proc. of ICSE Workshop on Software EngineeringChallenges of Cloud Computing, pp. 44-52, IEEEComputer Society Washington, DC, USA, May 2009.ISBN: 978-1-4244-3713-9.

[3]. Timothy Wood, PrashantShenoy, Alexandre Gerber,K.K. Ramkrishnan, Jacobus Van der Merwe, "TheCase for Enterprise-Ready Virtual Private Clouds",HotCloud'09 Proceedings of the 2009 conference onHot topics in cloud computing, San Diego, CA, USA,2009.http://www.usenix.

[4]. Hashizume et al. Journal of Internet Services and applications 2013, 4:5 www.jisajournal.com/content/4/1/5

[5]. Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[6].Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China.Springer-Verlag Berlin, Heidelberg

[7]. Centre for the Protection of National Infrastructure (2010) InformationSecurity Briefing 01/2010 Cloud Computing. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

[8]. Khalid A (2010) Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10), pp 278–281

[9]. Cloud Computing: Benefits, Risks and Recommendations for Information Security, ENISA Report, 2009, available at: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[10]. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance (CSA) Report, 2009, available at: www.cloudsecurityalliance.org/csaguide.pdf.

[11].Amazon Elastic Compute Cloud (Amazon EC2), http://aws.amazon.com/ec2/.

[12]. Hu, Y. C., Perrig, A, Johnson, D. B. (2003). SEAD: secure efficient distance vector routingfor mobile wireless ad hoc networks. Ad Hoc Networks, 1(1), 175-192.

[13]. Ioannidis, J., Bellovin, S. M. (2002). Implementing pushback: router-based defense againstDDoS attacks. Proceedings of NDSS.The Internet Society, Reston, VA.

[14]. Jian, W. (2000). A possible LAST_ACK DoS attack and fix. Available at:http://www.ussg.iu.edu/hypermail/linux/kernel/0004.1/0105.html. (Date of access: October31, 2006)

[15]. Jin, C., Wang, H., and Shin, K. G. (2003). Hop-count filtering: an effective defense againstspoofed DDoS traffic. Proceedings of ACM CCS, 30-41. ACM Press, New York.

[16]. Johnson, D., Maltz, D., Hu, Y. C., and Jetcheva, J. (2002) The dynamic source routingprotocol for mobile ad hoc networks (DSR). IETF Internet draft, draft-ietf-manet-dsr-09.txt.