International Journal of Computer Applications Technology and Research
Volume 3– Issue 8, 510 - 514, 2014, ISSN: 2319–8656

Information Security in Cloud Computing

E.Kesavulu Reddy
Dept.of Computer Science,
S.V.University College of CM & CS,
Tirupati, Andhra Pradesh, India-517502.

Abstract :-The National Institute of Standards and Technology (NIST) defined cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. Cloud Computing refers to the following concepts of Grid Computing, Utility Computing, software as a service, storage in the cloud and virtualization. These are termed as a client using a provider's service remotely, known as cloud. Cloud computing has the potential to change how organizations manage information technology and transform the economics of hardware and software at the same time. Cloud computing promised to bring a new set of entrepreneurs who could start their venture with zero investment on IT infrastructure. A principal goal of this paper is to identify privacy and security issues in the distributed environment and concern to cloud computing participants and users .

Keywords: Cloud computing, Security and Privacy, Information Technology, IT, Software as a service, Grid Computing, Utility Computing, Security.

1. INTRODUCTION

The Cloud Computing is a latest concept to become popular in computer industry. The basic idea of Cloud Computing is the sharing of computing resources among a community of users. At present cloud computing emerged as a web based technology computing that provides a freedom in the establishment of IT infrastructure[1]. Cloud is basically representing internet and web based applications. It basically works on user interactive software which is as simple as web browser. The various cloud vendors do not require their own infrastructure rather they can rent or use third party providers

2. DIFFERENT TYPES OF CLOUD COMPUTING

2.1. Cloud Computing

The Cloud Computing can be termed as internet based and are connected through the remote servers. Through this sharing of data processing tasks, online access to computer resources or services and centralized data storage. The best examples are electric station, in which consumer use power without having the knowledge of infrastructure to provide the service. In the same manner, the cloud vendors use the resources as a service and pay only for resources that they use. majority cloud computing infrastructures includes services delivered through common centers and build on servers.

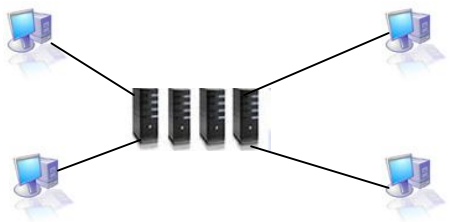


Fig.1.1. Cloud Containing Servers

2.2.. Grid Computing

Grid computing attaches computers from multiple administrative spheres to reach a common goal for solving a single task. The strategies used by Grid computing are to use middleware to divide the pieces of program among several computers. It includes computation in a distributed fashion. Grid computing is providing the resources of many computers in a network to a problem at the same time to a scientific or technical problem that needs large number of computers processing or ease to access large amount of data.

2.3..Utility Computing

Utility computing is the packaging of computation resources, such as computation, storage and service as a metered service. This model has the benefit of lesser cost to get hold of computer resources. Utility computing can be same to some extent which has the features of very large computations or a sudden height of demand which are supported by a huge number of computers. Utility computing is having some features of virtualization, so the large amount of storage or computing power is utilized at a single time sharing computers.

3. SERVICES OF CLOUD COMPUTING

Cloud computing provides both the software and hardware services through or over the internet. The services are mainly classified into three categories[3]:-

3.1. Software as a Service (SaaS)

The SaaS allows a user to use the software or application as service on demand using the Internet.

3.2. Infrastructure as a Service (IaaS):

It allows a user to use IT infrastructure such as hardware, storage and networking components as a service. The user can access the operating system, storage and application.

3.3. Platform as a Service (PaaS)

The provider provides a platform for their own use and user.

4. CLOUD COMPUTING MODEL

4.1. Private Cloud

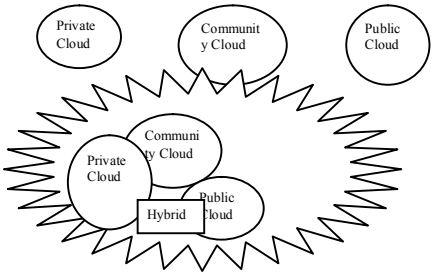
In this model, the infrastructure is used, maintained and operated for a specific company or organization.

4.2. Community Cloud

In this model, the infrastructure is shared among the various companies or organizations with similar areas of interests and requirements.

4.3. Public cloud

In this model, the infrastructure is available to the public for business purpose by various cloud service providers.



Flg.1.2. Cloud Computing Model

5. PRIVACY AND SECURITY ISSUES OF CLOUD COMPUTING

5.1. Privacy issues

1. Compelled Disclosure to the government Cloud can be subject to different levels of protection than on the information it contained
2. Data Security and Disclosure of Breaches: How does cloud provider protect customer's data how can customer ensure security compliance when storing information on the cloud?
3. Data Accessibility, Transfer and Retention: Can companies and consumers have access to data on cloud? [4]Can the data be destructed by cloud owners or should it be returned to customers?
4. Location of Data : The physical location of the server storing the data may have legal implications

5.2. Security issues

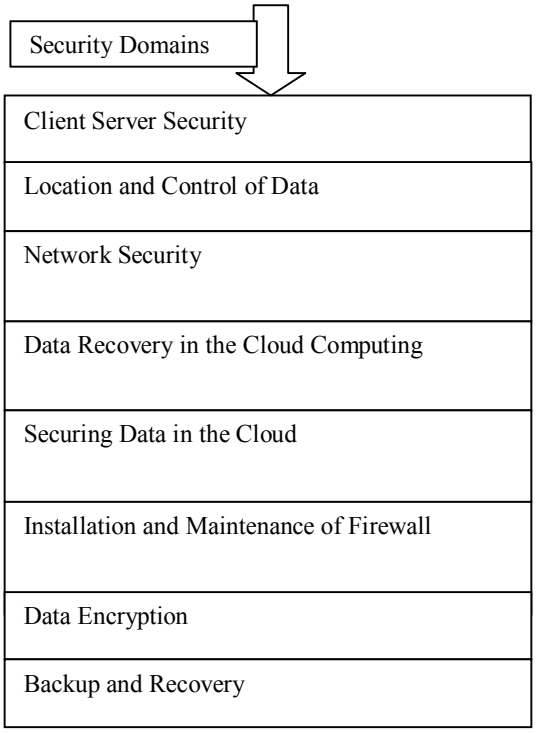


Fig.1.3. Security Domains

5.2.1. Client server security

Cloud computing encompasses a client and a server. To maintain secure client, organizations should review existing security practices and employ additional ones to ensure the security of its data. Clients must consider secure VPN to connect to the provider.

Web browsers are used in client side to access cloud computing services. Cloud providers usually provide the consumers with APIs which is used by the latter to control, monitor the cloud services. It is vital to ensure the security of these APIs to protect against both accidental and malicious attempts to evade the security. The various plug-ins and applications available in the web browsers also causes a serious threat to the client systems used to access the provider. Many of the web browsers do not allow automatic updates which will append to the security concerns. Cloud providers should also incorporate these measures to assure secure transaction among its customers

5.2.2. Location and control of data

In traditional data centers business had the privilege to know about the data flow, exact data location, precautions used to protect data from unauthorized access. The physical location' raises the question of legal governance over the data. Another impediment issue is incase of disputes arises between the provider and the customer.

Public cloud has the attraction of cost saving and low maintenance but the enticement comes with a drawback. The

infra structure has to be shared with unknown people. A cyber invader can act as a subscriber and can spread malicious viruses in the system. It is a responsibility of the provider to check the authenticity of the consumers. The vendor may grant some privileged third parties access to your stored data. The identity of such parties, if any, must be disclosed to the customer. Here, the third party could be a legal authority or even an internal employee. The customer should always be informed before the vendor allows third parties to access the stored data. Non cloud services also have security concerns but cloud has additional risk of external party involvement and exposure of critical and confidential data outside organizations control. Modifying security measures or introducing pristine Cloud provider stores the data in provider's side and maintenance is exclusively done by the providers, hence the clients have no means to check on the providers security practices, providers employees, their skills specializations etc.

5.2.3. Network security

Public cloud services are delivered over the internet, exposing the data which were previously secured in the internal firewalls. Applications which people used to access within organizations intranet are hence exposed to networking threats and internet vulnerabilities which includes distributed denial of service attacks, phishing, malwares and Trojan horses. If an attacker gains access to client credentials, they can eavesdrop on all activities and transactions, manipulate data, return falsified information, and redirect clients to illegitimate sites.

5.2.4. Data recovery in cloud computing

Usually cloud users do not know their data location and the vital query of data recovery in all circumstances may not be possible. The difficulty in retrieving data if there is a change in provider or a need to roll to different platform adds to the apprehension to embrace cloud computing.

5.2.5. Securing data in the cloud

A Proper implementation of security measures is mandatory in cloud computing. The fact that application is launched over the internet makes it susceptible for security risks. Cloud providers should think beyond the customary security practices like restricted user access, password protection etc. Physical location of stored data is also vital and it's the responsibility of the provider to choose the right location of storage.

5.2.6. Installation and maintenance of firewall

Installation of firewall and its maintenance is mandatory to ensure the protection. A firewall should be present in all external interfaces. Assessment of firewall policies and rule sets and reconfiguration of router should be done in regular intervals. Build and deploy a firewall that denies access from untrusted sources or applications, and adequately logs these events. Build and deploy a firewall that restricts access from systems that have direct external connection and those which contain confidential data or configuration data.

5.2.7. Data encryption

Data encryption is one common approach the providers to protect their clients data but the question is whether the data is getting stored in encrypted format or not. Many providers follow private/public key encryption to ensure data security. To store crucial data organizations can think of private or hybrid cloud where the data will be in secure corporate firewall.

5.2.8. Back up and recovery

In cloud computing data is stored in distributed location.. Backup software should include public cloud APIs, enabling simple backup and recovery across major cloud storage vendors, such as Amazon S3, Nirvanix Storage Delivery Network.

It is critical for the backup application to encrypt confidential data before sending it offsite to the cloud, protecting both data-in-transit over a WAN to a cloud storage vault and data-at-rest at the cloud storage site. Consumers need to verify that the cloud backup software they choose is certified and compliant with the Federal Information Processing Standards (FIPS) 140 requirements issued by the National Institute of Standards and Technology.

6. ENSURING SECURITY AGAINST THE VARIOUS TYPES OF ATTACKS

Problems associated with the network level security comprise of: DNS attacks, Sniffer attacks, issue of reused IP address, Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) etc.

6.1. DNS attacks

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be insufficient when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems..

6.2. Sniffer attacks

A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network.

6.3. Issue of Reused IP Addresses

Each node of a network is provided an IP address. IP address is basically a finite quantity. A large number of cases related to re-used IP-address issue have been observed lately. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. We can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user. It is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user.

6.4. DBGP Prefix Hijacking

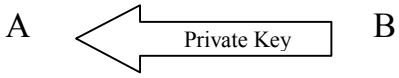
Prefix hijacking is a type of network attack in which a wrong announcement related to the IP addresses associated with an Autonomous system (AS) is made malicious parties get access to the untraceable IP addresses. On the internet, IP space is associated in blocks and remains under the control of AS's. An autonomous system can broadcast information of an IP contained in its regime to all its neighbours. These ASPs communicate using the Border Gateway Protocol (BGP) model. Sometimes, due to some error, a faulty AS may broadcast wrongly about the IPs associated with it[7]. In such case, the actual traffic gets routed to some IP other than the intended one. Hence, data is leaked or reaches to some other destination that it actually should not.

7. SECURITY AGAINST THE VARIOUS TYPES OF ATTACKS

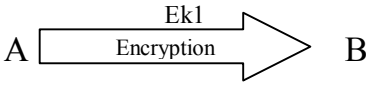
7.1. Symmetric Key Cryptography

It is equally important to secure the data in transit and security of transmitted data can be achieved through various encryption and decryption schemes. In such a scenario, even if the data gets into the hands of a hacker, he won't be able to make any unauthorized use until he knows how to decrypt it. A few of the encryption-decryption techniques include private and public key encryption. In a symmetric key (private key) encryption such as: DES, Triple DES, RC2, RC4 etc, the same key is used for encryption and decryption. Before the data is transferred, the key is shared between both the receiver and the sender. Sender then sends the data after having encrypted it using the key and the receiver decrypts it using the same key.

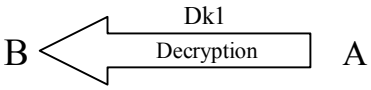
Step.1. Receiver sends its Private Key to sender



Step.2. Sender encrypts the Data using sender's Private key and sends it to Receiver



Step.3. Receiver using his Private Key and Decrypts the same data



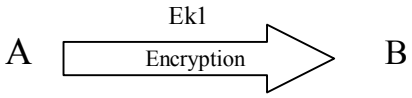
7.2. Asymmetric Key Cryptography

In case of Asymmetric key algorithm (RSA, DSA etc..) there are two types of keys known as Public Key and Private Key. Public key is common for both sender and receiver and the Private Key is used for decrypts the data from the sender

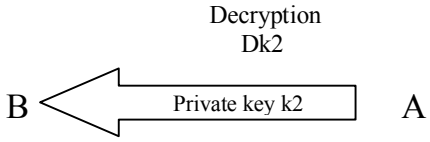
Step.1. Receiver sends its Public key to sender

In Public key encryption bit processing time is more than private key encryption,. But the security is more concern rather than the speed, public-key encryption provides more secure data transmission in comparison to private-key encryption. Security issues in a virtualized environment wherein a malicious virtual machine tries to take control of the hypervisor and access the data belonging to other [8].

Step.2. Sender encrypts the Data using sender's Public Key and sends it to Receiver



Step.3. Receiver using his Private Key and Decrypts the same data



8. CHALLENGES OF CLOUD COMPUTING

8.1. Data Security

Security is the main area of concern. A cloud vendor watches the usage of the cloud and the data. The person who is using the cloud doesn't have the knowledge about the back-end data storage. The user doesn't have the fair idea where they are storing their data. This can be rectified if vendors can provide a good security[7] or strong firewall and if they adopt encryption facility.

8.2. Data Recovery and Availability

This challenge is faced by the vendors. The vendor should maintain a good recovery system and good maintenance management system.

8.3. Management Abilities

The management of platform and communication are in its starting phase. There is a huge requirement to improve on the scalability and load equal balancing features.

9. ADVANTAGES OF CLOUD COMPUTING

- Cost Benefits
- Flexibility
- Reliability
- Maintenance
- Mobile Accessibility

10. CONCLUSION

Cloud computing is artifact of highly advanced research done for virtualization, distributed computing with usages of software

and its related services and also networking. It completely opens a new advanced and secured world of occasions for businesses, but mixed with the offers and high level of security challenges that needs to be definitely considered when society using the advanced cloud computing concepts. We are presenting the various hidden security challenges to be precisely and closely monitor. In this paper we are also discussed the intrinsic use of virtual systems as a tool for implementing an improved and advanced cloud environment.

11. REFERENCES

[1] Anderson, D., Frivold, T. & Valdes, A (May, 1995). Next generation Intrusion Detection Expert System (NIDES):

[2] Pant Durgesh, Sharma M.K "Cloud Computing "CSICommunication-2009",Vol-32, pp10-13

[3] George Reese. Cloud Application Architectures "Building Applications and Infrastructure in the Cloud" (Theory in Practice)

[4] Esteves, R.M. and Chunming Rong (2010), Social Impact of Privacy in Cloud Computing In 2010 , IEEE Second International Conference on Cloud Computing Technology and Science Nov. 30-Dec. 3 ,2010, pp. 593-596.

[5] Mell, P. and Grance, T. (2011) The NIST Denition of Cloud Computing (Draft): Recommendations of the National Institute of Standards and Technology. Special publication 800-145 (draft), Gaithersburg (MD).

[6] In Gutwirth, S., Poullet, Y., de Hert, P., and Leenes, R.,editors, Computers, Privacy and Data Protection: an Element of Choice, Springer,pages 293–314.

[7] Lin, G., D. Fu, J. Zhu and G. Dasmalchi (2009). Cloud Computing: IT as a Service. IT

[8] Weinhardt C., A. Anandasivam, B. Blau and J. Stosser (2009), Business Models in the Service World, IT Professional, Vol. 11 No 2, pp. 28-33