A SCRUTINY TO ATTACK ISSUES AND SECURITY CHALLENGES IN CLOUD COMPUTING

Subramaniam.T.K[1*], Deepa.B[2]

[*1]M.E.Scholar, Department of Computer Science & Engineering Nandha Engineering College, Erode, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India

ABSTRACT

Cloud computing is an anthology in which one or more computers are connected in a network. Cloud computing is a cluster of lattice computing, autonomic computing and utility computing. Cloud provides an on demand services to the users. Many numbers of users access the cloud to utilize the cloud resources. The security is one the major problem in cloud computing. Hence security is a major issue in cloud computing. Providing security is a major requirement of cloud computing. The study enclose all the security issues and attack issues in cloud computing.

KEYWORDS

Grid computing, autonomic computing

1. INTRODUCTION

Cloud computing other wise said to be an on-demand computing. Cloud computing is one of the types of Internet-based computing in which sharing of cloud resources, data and information. Normally data and programs are run on individual desktop computers. Instead these are run on cloud environments. Cloud computing provides platform, communications services and end user application services. The Cloud computing plays a vital role in IT industry [1]. The network of networks gives a remote access to set of resources that would be a decentralized. Cloud computing is flexible, multi-tendency and scalable. In this study the section 2 provides a deployment model of cloud computing, section 3 provides security challenges in cloud computing and attack issues.

2. CLOUD SERVICE MODEL

Cloud computing connect delivering computing resources such as remote servers machines, data storages space, and cloud users applications are services to end users by cloud computing service supplier. End users access on-demand cloud services via web browsers. Cloud computing service providers propose specific cloud services and make sure the significance of the services. Essentially, cloud computing consist of three layers: the system layer, the middle layer or platform layer, and the top layer or application layer.

DOI:10.5121/ijasa.2016.4101

The bottom layer

The bottom layer is the system layer, which comprise of additional resources such as communications of servers, network devices, and memory storage. It is said to be Infrastructures-a-service (IaaS). The computational resources are prepared and accessible for users as on-demand services [2]. With the exploit of virtualization technology, IaaS also offer virtual machines that allow clients to build composite network infrastructures. This model not only diminish the cost in importing physical apparatus for commerce, it also reduces the weight load of computer network administration since IT professionals are not essential to frequently monitor the health of physical network resources. The examples of a cloud computing service supplier of IaaS are Amazon's EC2. It offers a virtual computing environment with web service interfaces. By using the boundary, users can deploy Solaris or Windows based virtual machines, Linux, and execute their own tradition applications.

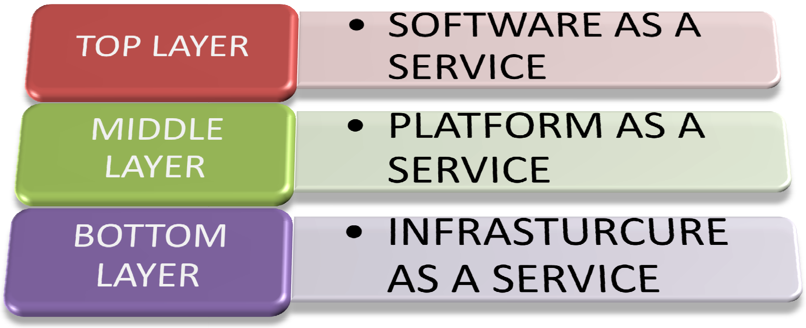

Fig: cloud service Deployment Model

The middle layer

The middle layer is the platform layer and is said to be a Platform-as-a-Service (PaaS). It is planned to supply a development platform for users to design their explicit applications. Middle layer services offers by this cloud model contain tools and libraries for application enlargement, permit users to have organized over the application deployment and configuration settings. With Platform-as-a-Service model, programmers are not necessary to obtain software development tools, therefore dropping the cost of buying tools. Google Apps is an example of Platform- as-a-Service model it is a suite of Google tools that comprises Google Talk, Gmail, Google Groups, Google Docs, Google Calendar, and Google Sites. It permits users to modify these tools on their own domain names [1][2]. Windows Azure is another Platform-as-a-Service provider. It enables users to construct own applications using various languages and domains, tools or frameworks. Users can then incorporate the applications into their presented IT environments.

The top layer

The top layer is the application layer, also called as Software-as-a-Service (SaaS). This layer permits users to lease applications runs clouds as a substitute of paying to purchase these applications. Because of its ability to decrease costs. Software-as-a-Service is popular in the middle of companies that install their businesses. Group on is an example that uses Software-as-a-Service. With the use of the online bearer solutions provided by Zendesk, Groupon processes its thousands of daily customer tickets more efficiently.

2.1. Benefits Of Cloud Computing

Reduced IT costs

Moving to cloud computing may diminish the cost of running and preserve IT systems. Rather than acquire costly systems and equipment for your business, cloud computing can decrease the costs by using the resources of cloud computing service supplier. It may be able to diminish the working costs because: the cost of system upgrades, original hardware and software may be built-in in the agreement; cloud computing no longer need to pay wages for expert staff, the energy utilization costs may be condensed, there are fewer time delays.

Scalability

The business can scale up or scale down the procedure and storage desires quickly to suit situation, permit flexibility as needs change. Rather than purchase and install expensive upgrade in individual computer, cloud computer service provider can handle this all works. Use the cloud frees up the moment so we can get on with managing business.

Business continuity

Defending data and systems is an imperative part of business durability development. Whether experience a natural tragedy, power collapse or other predicament, encloses the data accumulate in the cloud environments ensure that it is backed up and confined in a secure and safe position. Being able to right to use data again rapidly permit conducting business as usual, minimizing any downtime and overcome of productivity.

Collaboration effectiveness

Collaboration in a cloud computing environment gives the business capacity to commune and share more easily external of the traditional communication methods. If cloud computing operating on a project across different locations, might use cloud computing to provide employees, contractors and third parties admission to the equal files. The cloud users choose a cloud computing representation that formulates it easy for to share your report with adviser.

Flexibility of work practices

Cloud computing allow employees to be more stretchy in their work practices. For example, they have the ability to access data from home, on holiday, or via the convert to and from work. If need admission to data while off-site, can connect to useful office, quickly and easily.

Cost Savings

Perhaps, the most important cloud computing advantages is in terms of IT expenditure funds. Businesses, no issue with their type or size, exist to make money while keeping investment and operational expenses to a minimum. With cloud computing, you can save important capital costs with zero in-house server storage space and application requirements. The need of on-premises infrastructure also removes their related operational costs in the forms of bandwidth and power supply, air provision for server rooms and management costs.

Manageability

Cloud computing provides enhanced and basic IT management and maintenance capabilities through central management of resources, vendor managed infrastructure and Service Level agreements. IT communications updates and continuance are eliminating, as all the cloud computing resources are maintained by the service provider. A simple web-based user interface for access software, applications and services need not to installation and a Service Level Agreement ensures the timely and assured delivery, management and maintenance of IT services.

3. Security Challenges

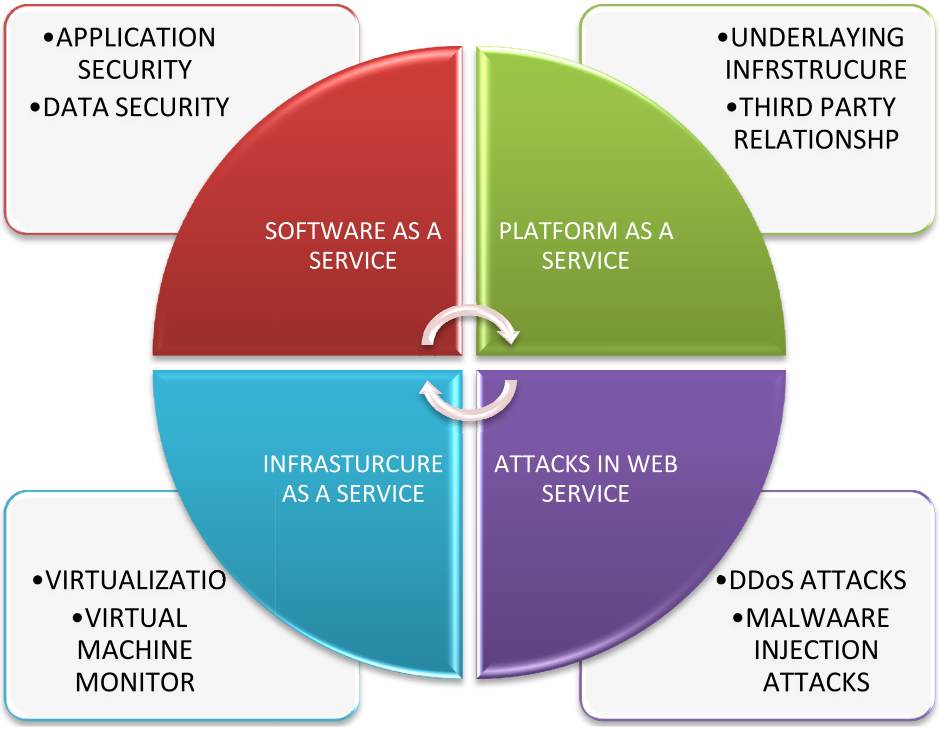

Fig: Security Challenges in cloud

3.1. Security Issues in Software as a Service

Software-as-a-Service offers application services on demand such as electronic mail, audio and video conferencing software tools, and business specific applications such as ERP, CRM, and SCM. Software-as-a-Service users have fewer controls over security among the three fundamental delivery representations in the cloud [3]. The adoption of Software-as-a-Service applications may raise some security concerns.

3.1.1.1. Application Security

These application requests are usually transport to the user via the Internet through a Web browser. However, blemish in web applications may generate vulnerabilities for the Software-as-a-Service applications [4][5]. The botnets in the network may create malicious activities Security challenges in Software-as-a-Service applications are same as that of web application technology, but conventional security solutions does not successfully protect it from malicious attacks[8]. The Open Web Application Security Project (OWASP) has recognized the ten most critical web applications security threats.

3.1.1.2 Multi-Tendency

Multi-tenancy is a structural design in which a distinct instance of a software application provides numerous customers. Each customer is said to be a tenant. Tenants may be given the capability to modify some parts of the application, such as colour of the graphical user interface or it may with business rules, but they not able to customize the application's code [10]. Software-as-a-Service applications can be clustered into development models that are resolute by the following characteristics: with metadata it is configurable and also it is configurable.

In the architectural model, each and every client has individual customized instance of the software application. This architectural model has disadvantages, but security issues are less when compared to other models. In the next maturity model, the dealer also supplies different instances of the applications for each and every customer, but all the instances use the same application code. In this maturity model the customers can customize some configuration options to satisfy their needs. In the last maturity model multi-tenancy is appended, so that single instances that serves all customers [9]. This approach facilitates more efficient use of the resources but scalability is restrictive. Since the data sources from multiple tenants are likely to be stored in the same database. Security mechanism policies are required to guarantee that customer’s data are kept take apart away from other customers.

3.1.3 Accessibility

Accessing applications over the internet are shared via users through web browser. This allow user to makes access from any network connected devices easier. It also includes public computers devices, remote and mobile devices. It also exposes the service to extra security risks. The Cloud Security Alliance [10] has discharged a document. The document that explains the present state of mobile computing and the threats in this area such as information pinching mobile malware devices, insecure wireless networks, vulnerabilities originate in the device Operating System and official business applications, and proximity-based hew.

3.2. Platform-as-a-service security Issues

Platform-as-a-service provides facilitates for deployment of cloud-based applications without the charge of importing and maintaining the underlying hardware platforms and software layers [11]. As with Software as a Service and Infrastructure as a Service, Platform as a Service depends on a protected and trustworthy network and secure web browser applications. Platform as a Service application security covers two software layers. That includes Security of the platform itself that is runtime and engine. Security of customer applications implemented on this platform [10]. This is responsible for protected the platform software stack from attacks and other security issues.

3.2.1. Third-party relationships

Platform as a Service provides a traditional program Languages, software platforms to end user. This also provides a third-party web services components such as mashups [11]. Mashups application combine more than one source element into a single incorporated unit. This also has security related to issues. In this platform user has to depend on security of web hosted tools and also depends on third party security issues.

3.2.2. Infrastructure security

In Platform-as-a-service, programmers and developers do not access to the underlying infrastructure layers, so clod service providers are only responsible for securing their underlying infrastructure layers as well as the end user applications services [12]. Even though developers and programmers are in control of the securing their applications, they do not have the guarantee that the maturity environment tools provided by a Platform-as-a-service provider are secure.

3.3. Infrastructure as a service security Issues

Infrastructure as a Service provides a number of resources such as web servers, data storage space, networks, and other resources necessary for computing .These of connected in the form of virtualized systems. These virtualized system are accessed through internet [13] .The user of system can run any software and application with control over with allocated virtual resources. They need to control the running software and configure the security policies.

3.3.1. Virtualization

Virtualization allows users to run a variety of applications and also it allow user create and share virtual machines. These virtual machines are more vulnerable to the environment. The attackers can attack the target system easily with help of new virtual machines .The new virtual machines can easily deployed in cloud environments. This is complex to provide a security to physical machine rather than virtual machines. This system will be more vulnerable to all types of security attacks. Providing security to virtual machines is a challenge task.

3.1.2 Virtual machine monitor

The Virtual Machine Monitor (VMM) or hypervisor is answerable for virtual machines separation. Therefore, if the Virtual Machine Monitor is compromised, its virtual machines may potentially be compromised as well. The Virtual Machine Monitor is low-level software application. That software application manages and monitors all the virtual machines in cloud environment. To make it secure keep the virtual machines as simple and use small virtual machine software application [14]. This virtualization can reduce fault tolerance and maintains a load balancing. This virtualization also acts as a loop hole for attackers. The malicious virtual machine can attack other virtual machines. This is also a challenging task to provide security to virtual machines.

3.4. WEB SERVICE ATTACKS IN CLOUD

3.4.1 DDoS Attacks

DDoS attack is said to be a Distributed Denial of Service attack. In DDoS attack, the attacker tries to avoid the valid users to access the resources and services in the cloud environment. In this attack, the attacker send huge number of messages packets to the target server .The target server verifies each and every message packets. While verifying the requests message packets, it has returned invalid addresses.

While verifying requests packets, the server become over loaded. The attackers make the server to halt before finale the connection [17] [18]. When the request association is blocked by the server, the attacker sends more valid messages packets with invalid network addresses. This makes the network and to be server in a busy state and overloaded. This attack causes the network traffic and services are not available to the end users.

Malware Injection Attacks
DDoS Attacks
Phising Attacks

Fig : web service attacks in cloud

3.4.2. Malware Injection Attacks

In the cloud computing environment the client’s request is processed based on authentication and authorization, at that time there is a huge opportunity of Meta data switch over between the web server and web browser. An attacker can take advantage during this switch over time of metadata. During this time the attacker attempts to introduce a harmful code or any other service to cloud environment. This injected service or code which looks like a service that are already available in the cloud environments. Once the malicious code is injected in cloud, it will run continuously as a single instance. And it affects the cloud environments [15]. This will create a loop hole for attackers in cloud environments. It is one of the major security challenges in cloud.

3.4.3. Wrapping attacks

Wrapping attacks use XML signature wrapping to increase a weakness when web servers validate the signed requests [15]. The attack is done at the time of the translation of SOAP messages between a valid user and the web server. By replica the user's account and password in the login period, the hacker inserts a bogus element into the communication structure, shift the original message body under the wrapper that replaces the content of the message content with harmful code, and then sends the message packets to the server. Hence the original body is still valid; the server will be scam into approve the message that has actually been altered. As a result, the hacker is able to gain unauthorized admittance to secured resources and succession the proposed operations.

3.4.4. Phishing attack

Phishing is a way of rescue personal information from innocent user through sending emails, webpage linker and instant message. These links appear to the genuine but leads to false access locations. Phishing attacks are of two categories one is abuse behavior: an attacker multitudes a phishing attack site in the cloud computing environments by using cloud services [16]. Second one is hijack the accounts using social or public engineering technique. To avoid the phishing attacks admission to sensitive data about the enterprise. The client or employee passwords used to admittance the cloud should be strong password and hard enough to guess. This also one of the security challenges to cloud environment.

3.4.4. Stepping stone attack

Stepping stone attack the impostor attempt to access the data. The attacker hides their locations and their identity. This is not done by directly intruding in to target fatalities host by with help of series of other hosts called stepping Stone [16]. Stepping stone host is identified based on investigation of inward and leaving traffic through stepping stone host. This increase the network traffic and delay in network .This type of attack is more vulnerable to cloud environments.

4. CONCLUSION

Cloud Computing is a comparatively new technology that provides a good more numbers of benefits for its users. Cloud computing also economically profitable to the business people and IT industry .Simultaneously cloud computing also lift up some protection problems which may cause and down its use .Accepting and understanding the vulnerabilities, loop hole exist in Cloud Computing environment will help organizations and business, IT industry to make secure towards the Cloud environments. This survey discuss about security issues in cloud computing primarily concentrate on the security issues and vulnerabilities in the environments.

5. REFERENCES

[1] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N " Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom)," Beijing, China. Springer Berlin, Heidelberg, pp 347–358,2009.

[2]Zhang S, Zhang S, Chen X, Huo X "Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China" IEEE Computer Society, Washington, DC, USA, pp 93–97, 2010.

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

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

[5] Khalid A ," Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10),pp 27,2010.

[6] Mather T, Kumaraswamy S, Latif S ," Cloud Security and Privacy". O'Reilly Media, Inc., Sebastopol, CA,2009.

[7] Li W, Ping L " Trust model to enhance Security and interoperability of Cloud environment. In: Proceedings of the 1st International conference on Cloud Computing",. Springer Berlin Heidelberg, Beijing, China, pp 69–79,2009.

[8] Rittinghouse JW, Ransome JF,"Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press,2009

[9] Grobauer B, Walloschek T, Stocker E ,"Understanding Cloud Computing vulnerabilities." IEEE Security Privacy 9(2):50–57,2011.

[10] Subashini S, Kavitha V ,"A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1,2011.

[11] Onwubiko C," Security issues to Cloud Computing. In: Antonopoulos N, Gillam L (ed) Cloud Computing: principles, systems & applications. Springer-Verlag,2010.

[12] Morsy MA, Grundy J, Müller I ," An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia",2010.

[13] Jansen WA ," Cloud Hooks: Security and Privacy Issues in Cloud Computing. In: Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa", Kauai, HI. IEEE Computer Society, Washington, DC,USA, pp 1–10,2011.

[14] Zissis D, Lekkas D ,"Addressing Cloud Computing Security issues. Future Generations Computer System ",28(3):583–592,2012.

[15] Kazi Zunnurhain and Susan V. Vrbsky, "Security Attacks and Solutions in Clouds"2013.

[16] Apurva Shitoot, Sanjay Sahu, Rahul Chawda, "Security Aspects in Cloud Computing", IJETT, Volume 6 number 3 - Dec 2013

[17] Subramaniam.T.K, Deepa.B , "A Review towards DDoS Prevention and Detection Methodology" International Journal of Computational Science and Information Technology (IJCSITY) Vol.3,No.1/2/3,August 2015.

[18] Subramaniam.T.K, Deepa.B, "A Survey On DDOS Attack Detection And Prevention Methodology" International Journal of Intellectual Advancements and Research in Engineering Computations, JUNE 2015

AUTHORS

T.K.SUBRAMANIAM received the B.Tech degree in Information technology from Nandha Engineering College in the year 2014.He is currently doing h is M.E Computer science and Engineering in Nandha engineering college, Erode, India. His area of interest is web services. He has published many journal papers.

B.DEEPA received the M.E degree in Computer Science and Engineering from Nandha Engineering College in the year 2011.She is currently working as Assistant Professor in Nandha Engineering College, Erode, India. She has published many international and natioanal research papers. Her area is Network security and web services. She has depth knowledge of her research area.