International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

Cloud Computing and Its Issues

Rachita M V[1], Keerthana K N[2], M Sai Chakradhar Reddy[3], Nishanth Reddy Dasari[4]
[1]Assistant Professor, [2,3,4] Student,
Dept. of Computer Science,
Vemana Institute of Technology, Bangalore

Abstract *— **The term "cloud computing" is a recent buzz word in the IT world. Behind this fancy poetic phrase there lies a true picture of the future computing for both in technical perspective and social perspective. The cloud computing is aimed at providing IT has a service to the cloud users on demand basis with greater flexibility, availability, reliability and scalability with utility computing model. Clouds provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks such as: use of online storage space, implementation of business applications, development of modified computer software, and creation of a "realistic" network environment. In previous years, the number of people using cloud services has vividly increased and more data has been stored in cloud computing environments. In the meantime, data breaches to cloud services are also increasing every year due to hackers who are always trying to exploit the security weaknesses of the architecture of cloud. In this paper, three cloud service models were compared.***

Keywords*: Cloud computing, usage, advantages, applications, threats.*

I. INTRODUCTION

The last eras have protected the idea that information processing can be done more efficiently, on large farms of computing and storage systems accessible via the internet. Advancement in networking and other areas are answerable for the receipt of the two new computing models and led to the grid computing movement in the early 1990s and, since 2005, utility computing and cloud computing. Cloud computing is a path to utility computing embraced by major IT companies such as Amazon, Apple, Google, HP, IBM, Microsoft, Oracle and others. Cloud computing has been tangled in everybody's life. It provides applications and storage spaces as facilities over the Internet for little to no cost. Most of us utilize cloud computing services on a daily basis. For example, we use web-based email systems to exchange messages with others; social networking sites (e.g. Facebook, LinkedIn, Myspace, Twitter) to share information and stay in contact with friends; collaboration tools (e.g. Google docs) to work with people on the same document in real time. Cloud computing has also been involved in businesses; companies rental the services from cloud computing service suppliers to reduce operational costs and advance the cash flow.
There is no hesitation that the convenience and small cost of cloud computing services have changed our daily lives; however, the security issues associated with cloud computing make us susceptible to cybercrimes that happen every day. Hackers employ a variety of techniques to gain access to clouds without legal authorization or disrupt services on clouds in order to achieve exact objectives. Hackers could trick a cloud into treating their illegal activity as a valid instance, therefore, gaining unauthorized access to the information stored in the cloud. Hackers could also take advantage of the enormous computing power of clouds to fire attacks to users who are in the same or altered networks. For instance, hackers rented a server through Amazon's EC2 service and carried out an attack to Sony's PlayStation Network. Therefore, a good thoughtful of cloud security threats is necessary in order to provide more secure services to cloud users

II. CLOUD TYPES

It is an internet based computing where all the public resources, software and data are provided to the computers and devices. Users can access the information from anywhere and anytime.

Three types of clouds:

- Private cloud
- Public cloud
- Hybrid cloud

1. Private cloud:-This type of cloud is maintained within an organization and used solely for their internal persistence. So the utility model is not a big term in this situation.

2. Many companies are moving towards this setting and experts consider this is the first step for an organization to move into cloud. Security, network bandwidth are not serious issues for reserved cloud
3. Public cloud:-In this type an organization charges cloud services from cloud providers on demand basis. Services provided to the users using service computing model.
4. Hybrid cloud:-This type of cloud is composed of multiple internal or external clouds. This is the scenario when an organization to public cloud computing domain from its internal private cloud.

III. ADVANTAGES OF CLOUD

The advantages of using cloud services can be of technical, Architectural, business.

A. CLOUD PROVIDERS VIEW:

Most of the data centers today are underutilized they are mostly 15% utilized. These data centers need spare capacity that sometimes get in the server usage. Large companies having those data centers can easily rent those computing power to other organization and get income out of it and also make the resources available for running data center(like power) utilized correctly.Companies having large data centers have already organized the resources and to provide cloud services they would need very little investment and cost would be incremental.

B. CLOUD USER'S POINT OF VIEW:

1. *Cloud users need not to take care about the hardware and software they use and also they don't have to be nervous about maintenance. The users are no longer tied to someone traditional system.*
2. *Virtualization technology gives the illusion to the users that they are having all the resources existing.*
3. *Cloud users can use the resources on demand basis and pays as much as they use.so the users can plan well for reducing their usage to minimize their expenditure.*
4. *Scalability is one of major advantages to cloud users. Scalability is provided vigorously to the users. Users get as much resources as they need. Thus, this model perfectly fits in the management spikes in the demand.*

IV. AMAZON CLOUD COMPUTING

A. AMAZON EC2 AND S3 SERVICES:

It one of the biggest organization to provide infrastructure as a service. They provide the computer architecture with XEN virtual machine. Amazon EC2 is one of the biggest development of XEN architecture to date. The client can install their operating system on virtual machine. EC2 uses simple storage service (S3) for storage of data .users can hire suitable amount CPU power, storage and memory with any upfront commitment. Users can control the entire software stack from kernel upwards. The architecture has two components one is the EC2 for computing purpose and S3 is for storage purposes.

B. SIMPLE STORAGE SERVICE (S3):

S3 can be thought as a globally available distributed hash table with high level access control. Data is stored in name or value pairs. Names are like UNIX filenames and the value can be object having size up to 5GB with up to 4K of metadata for each object. All objects in amazon's S3 must fit in to the global name space. This name space consist of a "bucket name" and "object name". Bucket names are like user names in traditional mail account and provided by amazon on first come first serve basis. An AWS (amazon web services) account can have max of 100 buckets. Data to S3 can be sent by SOAP based (API) are with raw HTTP "PUT" commands. Data can be retrieved using SOAP HTTP or bit torrent. While using bit torrent the S3 system operates as both as tracker and the initial seeder. There are also some tools available which enables the users to view S3 as a remote file system. Upload download rate from and to S3 is not that much exciting .one developer from Germany reported experiencing 10 to 100 kbps. This rate can go up to 1 to 2 mbps on the advanced side depending on the time of the day although the speed is not that much fascinating it is good enough for backup purposes although for doing computation it is not suitable .

C. AMAZON ELASTIC COMPUTE CLOUD (AMAZON EC2):

As the name implies EC2 rents cloud of computers to the users with the flexibility of choosing the configuration of the virtual machine like RAM size, local disk, processor speeds etc.Machines that supply EC2 services are actually virtual machines on top of XEN platform. Users can store a disk image inside S3 and create a virtual machine in EC2 using tools provided by amazon. This virtual machine can be easily used using a java program and can also be monitored. As EC2 is based on XEN it supports any Linux distributed as well as other Oss. Amazon does not promise about trustworthiness of the EC2 computers. Any machine can crash at any moment and they are not backed up. Although these machine generally don't crash according to the experience of the users but it is safe to use S3 to store information which is more reliable and computer-generated service. EC2 security model is similar to that of S3. The only difference is that the commands are signed with an X 509 private key. But this key is downloaded from AWS account so the safekeeping depends fundamentally on the AWS username and password.

V. AMAZON EC2 BENEFITS

Web services which provides secure, resizable, computing capacity in the cloud. It is designed to make wed scale () cloud computing easier for developers. It provides complete control of the computing resources and allows to run on amazon proven computing environment.

Amazon EC2 reduces the time required to obtain and boot new server instances from hours to minutes, which allows to quickly scale capacity. Amazon EC2 can change the economics of computing by allowing to pay only for capacity that one can actually use it. Amazon EC2 provides developers the tools to build failure resilient applications and isolate them from common failure scenarios.

1. **ELASTIC WEB SCALE COMPUTING:**
Amazon EC2 enables us to increase or decrease capacity within minutes, hours, days. One can commission others, hundreds or even thousands of server instances simultaneously. Because all this are controlled by web service APIs.
2. **COMPLETELY CONTROLLED:**
One can have complete control on their instances including root access and the ability to interact with them as you would any machines. You can stop any instances while retaining the data on the boot partition, and then subsequently restart the same instance using web service APIs. Instances can be restarted remotely using web service APIs, and you also have access to their console output.
3. **FLEXIBLE CLOUD HOSTING SERVICES:**
You have the choice of multiple instance kinds, operating systems, and software packages. Amazon EC2 allows you to select a configuration of memory, CPU, instances storage, and the boot partition size that is optimal for your choice of operating system and application.
4. **INTEGRATED:**
Amazon EC2 is integrated with most AWS services such as amazon simple storage service (amazon S3), Amazon relational database service (amazon RDS), And the amazon virtual private cloud (amazon VPC) to provide a complete, secure solution for computing, query processing, and cloud storage across a wide range of applications.
5. **RELIABLE:**
Amazon EC2 offers a great reliable environment where replacement cases can be rapidly and predictably commissioned. The service runs within amazon's proven network infrastructure and data centers.
6. **SECURE:**
Cloud security at AWS is the highest priority. As an AWS customer, you will benefit from a data center and network architecture built to meet the requirement of the most security sensitive organizations.
7. **INEXPENSIVE:**
Amazon EC2 passes on to you the financial benefits of amazon's scale. You pay a very low rate for the compute capacity you actually consume.
8. **EASY TO START:**
There are several ways to get started with in Amazon EC2. You can use the AWS management console, the AWS command line tools (CLI), or AWS SDKs. AWS is free to get started.

VI. CLOUD SECURITY ATTACKS

A. MALWARE INJECTION ATTACK:

Web-based applications provide dynamic web pages for Internet users to access application servers via a web browser. The applications can be as simple as an email system or as complicated as an online banking system. Study has shown that the servers are vulnerable to web-based attacks. According to a report by Symantec, the number of web attacks in 2011 increased by 36% with over 4,500 new attacks each day. The attacks included cross site scripting, injection flaws, information leakage and improper fault handling, broken validation and session management, failure to restrict URL access, improper data validation, insecure communications, and malicious file execution. Malware injection attack is one category of web-based attacks, in which hackers exploit vulnerabilities of a web application and embed malicious codes into it that changes the course of its normal execution. Like web-based applications, cloud systems are also susceptible to malware injection attacks. Hackers craft a malicious application, program, and virtual machine and inject them into target cloud service models SaaS, PaaS and IaaS, respectively. Once the injection is completed, the malicious module is executed as one of the valid instances running in the cloud; then, the hacker can do whatever s/he desires such as eavesdropping, data manipulation, and data theft.
Among all of the malware injection attacks, SQL injection attack and cross-site scripting attack are the two most common forms. SQL injection attack increased 69% in Q2 2012 than Q1 comparatively, According to a report by secure cloud host provider Fire Host. Fire Host said that between April and June, it blocked nearly half-million SQL attacks.

SQL injections goal SQL servers that run vulnerable database applications. Hackers exploit the vulnerabilities of web servers and inject a malicious code in order to bypass login and gain illegal access to backend databases. If successful, hackers can manipulate the contents of the databases, retrieve confidential data, remotely execute system commands, or even take control of the web server for further criminal activities. Sony's PlayStation was a victim of an SQL injection attack. Sophos Labs blog reported that an SQL injection attack has been successfully used to plant unauthorized code on 209 pages promoting the PlayStation games, "Sing Star Pop" and "God of War". SQL injection attacks can be launched by a botnet. The asprox botnet used a thousand bots that were equipped with an SQL injection kit to fire an SQL injection attack. The bots first sent encoded SQL queries containing the exploit payload to Google for searching web servers that run ASP.net. Then, the bots started an SQL injection attack against the web sites returned from those queries. Overall, approximately 6 million URLs belonging to 153,000 different web sites were victims of SQL injection attack by the Asprox botnet.

A scenario that demonstrates SQL injection attacking cloud systems was illustrated in. An online retail SaaS application that allows multiple retailers to host their products and sell them through SaaS was used. The procedure of exploiting vulnerability and accessing to backend database was explained in details. Cross-site scripting (XSS) attacks are considered one of the most malicious and dangerous attack types by Fire Host. 27% of web attacks, cross-site scripting attack, were successfully blocked from causing harm to Fire Host clients' web applications and databases during Q2 2012. For accessing to the victim's account or tricking the victim into clicking a malicious link. Researchers in Germany have successfully demonstrated a XSS attack against Amazon AWS cloud computing platform. The vulnerability in Amazon's store allowed the team to hijack an AWS session and access to all customer data. The data includes authentication data, tokens, and even plain text passwords.

B. WRAPPING ATTACK:

When a client desires services to a web server through a web browser, the service is interacted using Simple Object Access Protocol (SOAP) messages that are transferred through HTTP protocol with an Extensible Markup Language (XML) format. In order to ensure confidentiality and data integrity of SOAP messages in transit between clients and servers, a security mechanism, WS-Security (Web Services Security), for web service is applied. It make use of digital signature to get the message signed and encryption technique to encrypt the content of the message. This makes the client genuine and the server can validate that the message is not tampered with during transmission. Wrapping attacks use XML signature wrapping (or XML rewriting) to exploit a weakness when web servers validate signed requests. The attack is done during the translation of SOAP messages between a legitimate user and the web server. By duplicating the user's account and password in the login period, the hacker inserts a bogus element (the wrapper) into the message assembly, moves the original message body under the wrapper, replaces the content of the message with malevolent code, and then sends the message to the server. Since the original body is still valid, the server will be tricked into authorizing the message that has actually been altered. As a result, the hacker is able to gain illegal access to protected resources and process the intended operations.

Since cloud users normally request services from cloud computing service providers through a web browser, wrapping attacks can cause damage to cloud systems as well. Amazon's EC2 was discovered to be vulnerable to wrapping attacks in 2008. The research showed EC2 had a weakness in the SOAP message security validation mechanism. A signed SOAP request of a legitimate user can be intercepted and modified. As a result, hackers could take unprivileged actions on victim's accounts in clouds. Using XML signature wrapping technique, researchers also demonstrated an account hijacking attack that exploited vulnerability in the Amazon AWS. By altering authorized digitally signed SOAP messages, the researchers were able to obtain unauthorized access to a customer's account, delete and create new images on the customer's EC2 instance, and perform other administrative tasks.

REFERENCES

[1]. F.M.Aymerich, G. Fenu, and S. Surcis. An approach to a cloud computing network. Applications of Digital Information and Web Technologies, 2008. ICADIWT 2008., pages 113 –118, August 2008.
[2]. Simson L. Garfinkel. An evaluation of amazon's grid computing services: Ec2, s3 and sqs. Technical report, 2007.
[3]. S.L. Garfinkel. Commodity grid computing with amazon's S3 and EC2. https://www.usenix.org/publications/login/2007-02/openpdfs/ garfinkel.pdf, 2007.
[4]. Web Based Attacks, Symantec White Paper, February 2009.
[5]. Symantec Internet Security Threat Report, 2011 Trends, Vol. 17, April 2012.
[6]. P. P. Ramgonda and R. R. Mudholkar, "Cloud Market Cogitation and Techniques to Averting SQL Injection for University Cloud," International Journal of Computer Technology and Applications, Vol. 3, No. 3, pp. 1217-1224, January, 2012.
[7]. A. S. Choudhary and M. L. Dhore, "CIDT: Detection of Malicious Code Injection Attacks on Web Application," International Journal of Computer Applications, Vol. 52, No. 2, pp. 19-26, August 2012.
[8]. Web Application Attack Report For The Second Quarter of 2012 http://www.firehost.com/company/newsroom/web-application-attack-report-second-quarter-2012.
[9]. Visitors to Sony PlayStation Website at Risk of Malware Infection, July 2008. http://www.sophos.com/en-us/press-office/press-releases/2008/07/playstation.aspx
[10]. N. Provos, M. A. Rajab, and P. Mavrommatis, "Cybercrime 2.0: When the Cloud Turns Dark," ACM Communications, Vol. 52, No. 4, pp. 42–47, 2009.
[11]. S. S. Rajan, Cloud Security Series | SQL Injection and SaaS, Cloud Computing Journal, November 2010.
[12]. Researchers Demo Cloud Security Issue with Amazon AWS Attack, October 2011. http://www.pcworld.idg.com.au/article/405419/researchers_demo_cloud_security_issue_amazon_aw s_attack/.
[13]. M. McIntosh and P. Austel, "XML Signature Element Wrapping Attacks and Countermeasures," 2005 workshop on Secure web services, ACM Press, New York, NY, pp. 20–27, 2005.
[14]. N. Gruschka and L. L. Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," IEEE International Conference on Web Services, Los Angeles, 2009.

