[IDSTM: January 2017]
ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

CLOUD COMPUTING AND ITS SECURITY ISSUES: A SURVEY

Ritu Kadyan, Nupur Chugh, Aarchi Goyal
CSE, Ganga Technical Campus,India

ABSTRACT

Cloud computing is experiencing significant growth these days with rapid adoption among various regions around the world. But there are few issues comes with adoption such as security issues. Cloud computing must be safe enough so that one cannot lose its data saved on cloud. This survey paper based on study from various research papers which introduces cloud computing, its service models, its characteristics. This paper also features the various security issues and the ways to overcomes these issues and ensure the privacy and prevention of data loss.

Keywords-. *Cloud, Security, Privacy.*

Introduction

Cloud computing is pretty big and it's growing bigger day by day. Unlike traditional computing where data is stored on your PC's local hard drive, the data in the cloud is stored on many physical and/or virtual servers that are hosted by a third-party service provider.

The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN.

Cloud Computing refers to manipulating, configuring, and accessing the hardware and software resources remotely. It offers online data storage, infrastructure, and application. Cloudcomputing is a model for delivering information technology services in which resources are retrieved from the internet through web based tools and applications, rather than a direct connection to a server. Cloud Computing is the use of hardware and software to deliver a service over a network (typically the Internet).

HISTORY OF CLOUD COMPUTING

The concept of Cloud Computing came into existence in the year 1950 with implementation of mainframe computers, accessible via thin/static clients. Since then, cloud computing has been evolved from static clients to dynamic ones and from software to services.

BASIC CONCEPTS

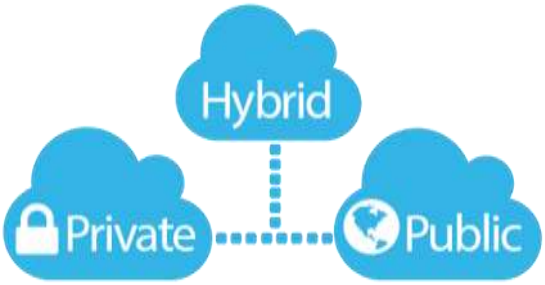
There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

Deployment Models

These models defines the type of access to the cloud i.e. How the cloud is located? Cloud can have any four type of access which are Public, Private, Community and Hybrid.

- Public cloud is easily accessible to general public. It is less secure due to its openness.
- Private cloud is accessible to an individual organization. It is more secured due to its private nature.
- Community cloud is accessible by the group of organizations.
- Hybrid cloud is a mixture of both public and private cloud. The critical activities are performed using private cloud and non-critical activities are performed using public cloud.

ISSN 2348 – 8034
Impact Factor- 4.022



Software ModelsThere are three ways to cloud compute. The three building blocks of cloud computing are:

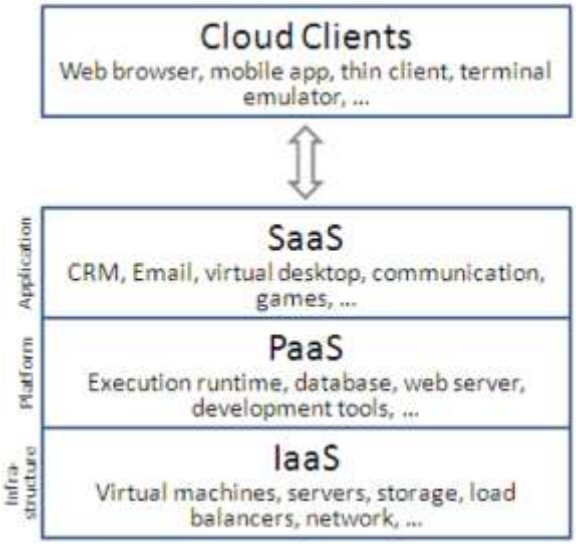
- Software as a Service or SaaS
- Platform as a Service or PaaS
- Infrastructure as a Service or IaaS

All of these allows users to run applications and stored data online however each offers a different levels of user flexibility.

a. Software as a Service (SaaS):From the complex to basic, cloud based applications called software as a service run on offsite computers that are owned and operated by others. User's computers connect to internet via a web browser to use the SaaS they've purchased.

b. Platform as a service (PaaS):It provides a cloud based environment that includes all the tools necessary for developing web-based applications. The cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting is minimized with this service option. When choosing PaaS, it is important to know what's included for free, how long a lock-in there is, if your security requirements are met and who are good-fit customers in terms of size and functionality.

c. Infrastructure as a Service: It provides companies with computing resources including servers, networking storage and data center space on a pay-per-use basis. The service provider owns the equipment and is also responsible for its maintenance and the client pays for use rather than up front so startup costs can be minimized.



ISSN 2348 – 8034
Impact Factor- 4.022

DRIVERS OF CLOUD COMPUTING

Cloud computing is rapidly growing area in IT security space because cloud architectures are popping up all over. The various cloud providers available in market are:

- Amazon: Amazon web services including the (EC2) Elastic compute cloud and (S3) Amazon simple storage device.
- Microsoft: Windows Azure Platform
- Google: Google App Engine
- IBM:Lotus Live(Platform as a Service)
- Salesforce:(Software as a Service)
- Rackspace cloud
- VMware

CHARACTERISTICS OF CLOUD COMPUTING

- On-Demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad Network Access: Capabilities are available over the internet and can be accessed through standard mechanisms that promote use by thin client platforms such as mobiles, tablets, laptops etc.
- Measured Service: Going back to the affordable nature of cloud, you only pay for what you use. You and your cloud provider can measure storage levels, bandwidth and number of users account and you are billed appropriately.
- Resource Pooling: The cloud computing enables users to enter and use the data in the cloud at the same time, from any location and at any time. This is an attractive feature for multiple business offices and field service that are usually outside the office.
- Rapid Elasticity: The cloud is flexible and scalable to suit your immediate business requirements. You can easily and very quickly add users and remove them, software features and other resources.

VARIOUS ISSUES IN CLOUD COMPUTING

Cloud computing is transforming the way we do business making IT more efficient and cost effective but it's also opening companies up to new types of cyber threats .
Data residency and Data security are the key concerns when moving to the cloud.
The main concerns with Data residency are:

- Who manages and have access to the data?
- Where is the data stored and what laws apply?
- Will you know the data is breached?
- Will data remain in the cloud even after termination of the service?

Data Encryption and Tokenization are the key solutions to overcome data residency concerns.

- Data Encryption is the mathematical process of converting clear text data into cypher text which cannot be read by anyone other than the customer who retains encryption key.
- In tokenization actual data resides locally in a token database. Randomly generated tokens are associated with the data and are sent to the cloud only be read by the custodian of the token database.

The significant differences between Tokenization and Encryption are:

- Tokenization protects only against external threats since anyone with access to the token database could access clear text data. It requires high capacity servers and database and more operational oversight to manage the critical token database that grows with increasing data volumes
- Encryption protects against internal and external threats since there is segregation of duties between where the keys are managed and where the encrypted data is stored. It requires light weight stateless servers with no data storage

The main concerns with data security are:

- Hijacking of Account: The growth and implementation of cloud in many organization has opened a new set of issues in account hacking. Attackers now have ability to use your login information to remotely access sensitive data stored on cloud, also attackers can falsify and manipulate information through hijacked credentials. InApril 2010 Amazonfaced a cross site scripting bug that targeted customer credentials as well. Phishing, key logging and buffer overflow all present similar types of threats.
- Data Breaches: A data breach is an incident in which our protected or confidential information is released, viewed, stolen or used by an individual who is not authorized to do so. The risk of data breach is not unique to cloud computing, but it consistently ranks as a top concern for customers of cloud. A cloud environment is subject to the same threats as a traditional corporate network as well as new avenues of attack by way of shared resources, cloud provider personal and their devices and third party partners of the cloud providers. Cloud providers are the highly accessible and the vast amount of data they host makes them an attractive target for the attackers.
- Insecure interfaces (UI) and APIs: Cloud computing providers expose a set of software user interfaces or application programming interfaces that customer use to interact with cloud services. Provisioning, management, orchestration and monitoring are all performed with the help of these interfaces. The security and availability of general cloud services is dependent on the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties may build on these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, because organizations may be required to relinquish their credentials to third parties in order to enable their agency. Generally, APIs and UIs are the most exposed part of a system, perhaps the only asset with an IP address available outside the trusted organizational boundary. These assets will be the target of heavy attack and adequate controls protecting them from the Internet are the first line of detection and defense.
- Exploited system vulnerabilities: System vulnerabilities or exploitable bugs in programs are not new, but they've become a bigger problem with the advent of multitenancy in cloud computing. Organizations share databases, memory and other resources in close proximity to one another, creating new attack surfaces fortunately, and attacks on system vulnerabilities can be mitigated with “basic IT processes,” says the CSA. Best practices include regular vulnerability scanning, prompt patch management, and quick follow-up on reported system threats. According to the CSA, the costs of mitigating system vulnerabilities “are relatively small compared to other IT expenditures.” The expense of putting IT processes in place to discover and repair vulnerabilities is small compared to the potential damage. Regulated industries need to patch as quickly as possible, preferably as part of an automated and recurring process, recommends the CSA. Change control processes that address emergency patching ensure that remediation activities are properly documented and reviewed by technical teams.
- Malicious insiders: A malicious insider threat to an organization is a former employee, contractor or other business partner who has authorized access to an organization’s network, system or data and intentionally exceeded or misused that access in a manner that negatively affected the integrity, confidentiality or availability of the organization’s information.
- Data loss: Data stored in the cloud can be lost for reasons other than malicious attacks. An accidental deletion of data by the cloud service provider, or a physical catastrophe such as a fire or earthquake, can lead to the permanent loss of user data unless the provider or cloud consumer takes adequate measures or steps to back up data. Amazon is an example of an organization that suffered data loss by permanently destroying many of its own customers’ data in 2011. Google was another organization that lost data when its power grid was struck by lightning four times. Securing the data means carefully reviewing the provider’s back up procedures as they relate to physical storage locations, physical access, and physical disasters.
- Denial of Service (DoS): Denial-of-service (DoS) attacks are attacks meant to prevent users of a service from being able to access their data or their applications. By forcing the targeted cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attackers, as is the case in distributed denial-of-service (DDoS) attacks—causes an intolerable system slowdown and leaves all legitimate service users confused and angry as to why the service is not responding.

ISSN 2348 – 8034
Impact Factor- 4.022

The above are some main security issues which comes when one moves to cloud computing.

DATA SECURITY AND PRIVACY IN CLOUD COMPUTING

Data security and privacy protection are two main factors of user's concerns about the cloud technology and becoming more important for the future development of cloud computing in business, industry and government. The different methods or techniques used to overcome these issues are:

- Confidentiality: Confidentiality is one of the most important security mechanisms for user's data protection in cloud computing. It mainly includes encryption of plain text into cypher text before the data stored in cloud. This technique protects the user data and even cloud service providers cannot read the content that is stored in this way in the cloud. This kind of protection is offered from Dell data protection and encryption. Waula cloud is another vendor which enables encryption for the data in the cloud.
- Access control: Access control is also very important security mechanism for enabling data protection in cloud. It ensures thatonly authorized users have access to the requested data. There are various techniques that enables proper access control to data stored in cloud. Intrusion detection systems, firewalls as well as segregation of obligations could be implemented on different layers of cloud. Firewall is enabling only content that is filtered to pass through the cloud network. Firewall is usually configured according defined security policies set by the users. Firewalls are usually related to Demilitarized zones (DMZ) which provide additional security. McAfee is a vendor that enables access control by offering different methods such as McAfee single sign on, McAfee web gateway, McAfee one time password.
- Authorization: It is very important for users in cloud computing when they login to some cloud service because it enables proves of their identity. So, authorization is usually employed after the authentication. Authorization in cloud is offered by VMware which integrate policies of service providers with the different policies and corporate directories. Oracle Database vault also enables authorization in cloud computing.
- Data recovery: It is very important that each system that is using cloud computing to has automatic backup procedure at least once in a week. The overall backup procedure should include the operating system, application software and data on the machine. Multiple backups over time could be implemented on machine which stores data.
- Boundary defense of the data in the cloud: Boundary defense in one Organization could be implemented by using commercial IDS and sniffers to detect attacks from external resources to the internal system of DMZ of the organization or vice versa. It also prevents from communication with known malicious IP address. Organization should include network based IPS devices as an addition to IDS to block known bad signatures or behavior of attacks. Only DMZ systems should communicate with private network systems of the organization via application proxies or application-aware firewalls over authorized channels. Anomalous activities could be easily detected if net flow collection and analysis to DMZ network is deployed.

CONCLUSION

In this paper we have discussed about cloud computing , its development and various characteristics of cloud. Cloud computing is used widely these days as it is flexible and cost efficient but there are some security issues in it which is the largest hurdle to leap. As our data is the matter of prime concern so here are some options to deal with it which we have find in our study that the main issues are like data centers security, insiders attack, virtualization, which are needed to be secure. We can secure them only if we focus on development of our cloud architecture for deterrent controls,detective controls, corrective controls and preventive controls.

REFERENCE

[1] Global Netoptex Incorporated. ―Demystifying the cloud.Important opportunities, crucial choices.‖ pp4-14. Available: http://www.gni.com [Dec. 13, 2009].
[2] Hanqian Wu, Yi Ding, Winer, C., Li Yao, ―Network Security for Virtual Machines in Cloud Computing,‖ 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30- Dec. 2, 2010. ISBN: 978-1-4244-8567-3
[3] Right Scale Inc., "Cloud Pricing Trends," White Paper, 2014

[4] EY, "Cloud Computing Adoption in India". Available at:http://www.ey.com/IN/en/Industries/Technology/Clou d-computing-adoption-in-India, Accessed 9 May 2015.
[5] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions," 7th International Conference on Informatics and Systems, pp. 1–8, 2010.
[6] R. Maggiani, Communication Consultant, Solari Communication, ―Cloud Computing is Changing How we Communicate‖, 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.
[7] V. Krishna Reddy, B. ThirumalRao, Dr. L.S.S. Reddy, P.SaiKiran ―Research Issues in Cloud Computing ― Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.
[8] K. Sun and Y. Li, "Effort Estimation in Cloud Migration Process," IEEE 7th International Symposium on Service Oriented System Engineering, pp. 84–91, 2013.
[9] B.P. Rimal, Choi Eunmi, I. Lumb, ―A Taxonomy and Survey of Cloud Computing Systems‖, Intl. Joint Conference on INC, IMS and IDC, 2009, pp. 44-51,Seoul, Aug, 2009. DOI: 10.1109/NCM.2009.218
[10] S. Wattal and A. Kumar, "Cloud Computing – An Emerging Trend in Information Technology," IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014.