A study on Issues and Challenges in Cloud Computing

Alka Chauhan
Assistant Professor, Department of Computer Science, D.M. College, Moga.

Received: September 15, 2018 Accepted: November 02, 2018

ABSTRACT: *Cloud computing is an Internet-based computing service provided by the third party allowing share of resources and data among devices.Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. . It provides lots of benefits such as simplicity and lower costs, almost unlimited storage, least maintenance, easy utilization, backup and recovery, continuous availability, quality of service, automated software integration, scalability, flexibility and reliability, easy access to information, elasticity, quick deployment and lower barrier to entry. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. . It provides lots of benefits such as simplicity and lower costs, almost unlimited storage, least maintenance, easy utilization, backup and recovery, continuous availability, quality of service, automated software integration, scalability, flexibility and reliability, easy access to information, elasticity, quick deployment and lower barrier to entry. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.*

Key Words: *Cloud Computing, Scalability, Infrastructure, IT.*

1. INTRODUCTION

Though the term Cloud Computing is not new now a day, let us have a definition of Cloud computing:"Cloud computing is a type of computing that provides simple, on-demand access to pools of highly elastic computing resources. These resources are provided as a service over a network (often the Internet), and are now possible due to a series of innovations across computing technologies, operations, and business models. Cloud enables the consumers of the technology to think of computing as effectively limitless, of minimal cost, and reliable, as well as not be concerned about how it is constructed, how it works, who operates it, or where it is located.For years the Internet has been represented on network diagrams by a cloud symbol until 2008 when a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing.. It help to increase the storage capacity because users can have more than one cloud service to stored their data and thus reduce the cost because there is no need to own an expensive computer with a larger memory. According to the US National Institute of Standards and Technology (NIST), cloud computing is a model enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. While the users are enjoying all the benefits that cloud computing could provide, many of the users did not realized that there are many threats that might cause a great loss them. Most of them did not even know how the cloud service provider manage their data and where exactly the data is stored. When choosing to use cloud computing service, the users are actually handling the confidential data to the third party who helps the users to keep and backup the data or resources. Based on that, there are some question that might be asked by the security professionals like "Do you really think that the data is safe and secure when it is managed by the third party?" and "Do you trust the cloud service that youuse?" Security issues and challenges are then arises since there is lack of awareness while the users are using the cloud service that provided by the cloud service provider

2. SECURITY ISSUES IN CLOUD COMPUTING

2.1 Cloud Deployments Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand as depicted in figure 2. The Cloud Computing model has three main deployment models which are:

2.1.1 Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that

emulate cloud The cloud infrastructure is owned by only one user and it is not shared with the others. The user has physical control over the cloud infrastructure and it is more secure compared to the public cloud where everyone share a same cloud infrastructure. It provides host services on private network that helps most corporate network and data administrators to become in-house service provider efficiently. Studies provides an insights of a private cloud that addresses the requirements and needs of e-learning and collaboration in university.

2.1.2 Public cloud

The entire infrastructure of this cloud model is located on the premises of the cloud service provider. The users normally share the same infrastructure pool with limited configuration. It is accessible by any user and any user can store their data in the same cloud provided by the cloud service provider. It provides scalable, dynamically provisioned and virtualized resources available over the Internet.

2.1.3 Hybrid cloud

Combination of the public, the private or even the community cloud infrastructure which allowed the transitive information exchange. It increased the flexibility of the cloud infrastructure where the users can implement the private cloud using the public cloud resources.

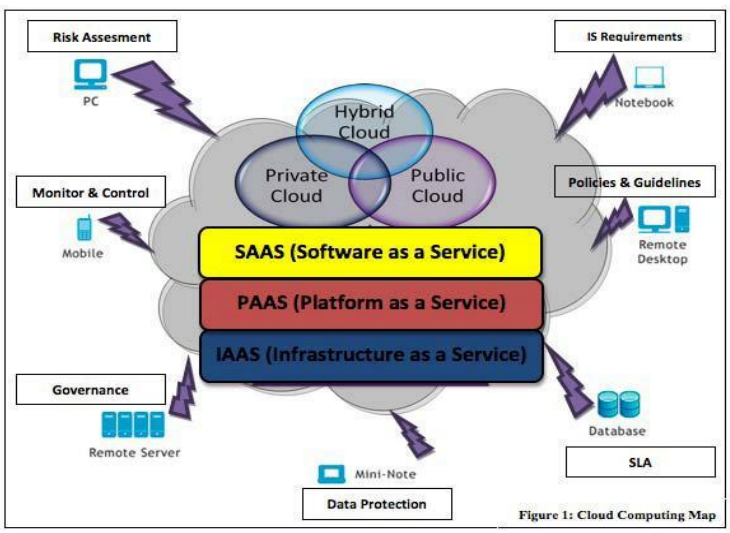

FIGURE 2: Cloud deployment model [13]

2.2 Cloud Computing Service Delivery Models

Following on the cloud deployment models, the next security consideration relates to the various cloud computing service delivery models. The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

2.2.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. The user allowed to rent the processing, storage and other fundamental computing resources to deploy and run arbitrary software which include operating system and applications and they have control over the operating system and network. It provides basic storage and computing capabilities. It also has a data centre space that can help to handle workload

2.2.2. Platform as a service (PaaS)

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS,middleware, etc. A middle layer of cloud service model that provides a software environment or platform for the users to design, develop, deploy and test their application without worrying about the underlying of the cloud infrastructure using the virtual servers of the cloud service provided [1,3]. Therefore, the users can build their own applications which running on the provider's infrastructure and they have control over the deployed application they built.

2.2.3 Software as a Service

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. It is the top layer of cloud service model. The cloud service provider developed and hosts the software or application on the cloud infrastructure allowing the users to use it with various devices by using the thin client interface such as web browser. However the underlying

cloud infrastructure, network, servers, operating systems or even individual application capabilities is not manageable by the users [3]. It helps the users to save cost because of licensing of the traditional packages is more expensive compared to the monthly fee for renting the application from options which are used in enforcing data protection transmitted over the Internet.[8]

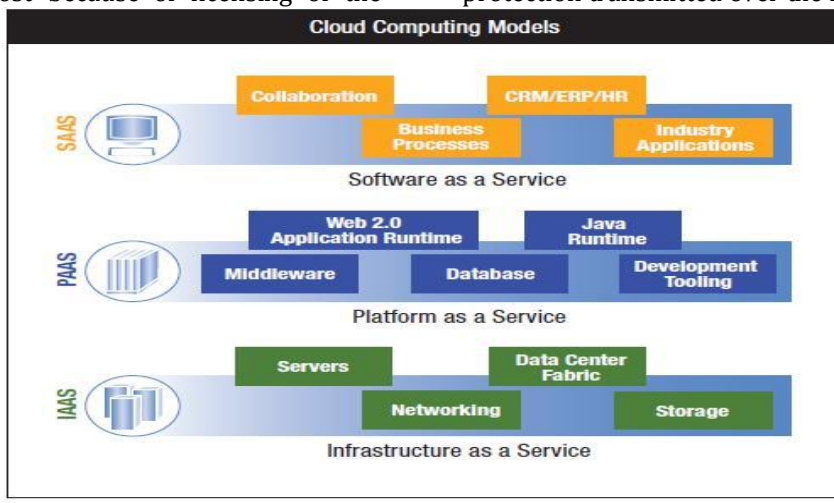

FIGURE 3: Cloud computing service delivery models

CLOUD COMPUTING CHALLENGES

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity., the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

A. Security: Data at rest is the major issues in cloud computing because users may store all their common, private, or even sensitive data in the cloud which can be accessed by anyone anywhere. Data theft is a very common issues that are facing by the cloud service providers nowadays. Besides, some cloud service providers even don't provide their own server because of the cost effectiveness and flexibility. There are also incidents like data loss which might be also a serious problem for the users. For example, the server is suddenly shut down and causes data loss of the users. Furthermore, natural disaster might also cause data to be damaged or corrupted. Therefore, physical data location can be considered one of the security issues in cloud computing.

B. Privacy: The cloud computing service provider must enforce their own policies to ensure the safety of the data users stored in their cloud model. They must make sure that they realize who is actually accessing the data stored in the cloud and only the authorized person can maintain the cloud service model [9]. The security of cloud computing should be done on the provider side and also the user side. Cloud service provider should provide a good layer of security protection for the users while the users should not tampered with the other user's data. The cloud computing is a good way to reduce the cost and provide more storage if and only if the security is done by both provider and user. [10] Claimed that regulatory reform is essential to protect sensitive data in the cloud since one of the most challenging aspect in cloud computing is to ensures that the consumer have trust in privacy and security of their data.

C. Threats issues:

There are lots of security issues regarding the cloud computing that have been widely used nowadays. There are top nine threat that pose severe danger to the cloud computing in year 2013 according to "The Notorious Nine: Cloud Computing Top Threat" by the Cloud Security Alliance (CSA) [11]. The top nine threat that have been mentioned in the white paper are:

i. Data Breaches

Data that stored to the cloud by the users might be important and sensitive. The data store in cloud might be stole by the unauthorized users and that might poses some level of danger to the users under attack. It is the top threat to threat to the cloud computing because hackers or attackers can easily access to the data of the users which store in the cloud. Data Loss

Data stored in cloud might be damaged or corrupted due to some reasons such as shut down of server because of financial or legal problem, natural disaster like earthquakes and fire [13]. Data might not be able to recover because back up is not done well and the data of the users will be

lost forever if there are no extra copies of that information.

ii. Account Hijacking

The user's account is stolen or hijacked and the hackers might impersonate he user to perform malicious and unauthorized activities which might also harm the user [14]. For example, the hackers might manipulate the data, provide false information and eavesdropping on transactions using the stolen account. In addition, no native APIs are used for login and anyone can register as a cloud service user hence the chances of the account being hijacked is high [15].

iii. Insecure APIs

Software Interface for the users to interact with the cloud services is also crucial to ensure the security of the cloud model. The API from the authentication and access control to the encryption and activity monitoring should be well implemented to protect against both accidental and malicious attack. For example, [16] propose two stage access control mechanism using the Role Based Access Control Model (RBAC) in order to provide a strong API mechanism.

iv. Denial of Service

Hacker use this type of attack to flood the machine or network resources of the cloud service provider which interrupt the users and prevent the users from connecting to the network access [11,17]. This is also a security issues that might harm the user because cloud service becomes unavailable to users and they might not get what they need in time.

v. Malicious Insiders

Employee of the company might also be a big threat. They might be the attacker themselves or a partner of the hacker who have the better chances of stealing or tampering the data of the cloud model with intention. These activities cause the sensitive or confidential data of the users leak to the others which might harm the targeted users. Studies by [18] reveals that password and other confidential data can be easily obtained by malicious insiders of cloud service providers. Studies by [19] addresses the problems of malicious insiders where they claimed that it should be studied in two context which are insider threat in cloud provider (i.e. insider is malicious employee working for cloud provider) and insider threat in cloud outsourcer (i.e. employee of an organization which sourced its infrastructure to the cloud).

vi. Abuse of Cloud Service

Most of the cloud computing systems have weak registration system. For example, anyone with a valid credit card may register and start using the cloud service immediately. Thus, attackers often conduct the malicious activities by abusing the relative anonymity of theregistration of the cloud computing services. Future areas of concern include password and key cracking, DDOS attack, launching dynamic attack points and hosting malicious data.

viii. Insufficient Due Diligence

Many users undertake little due diligence about their cloud service providers (CSPs). They did not even consider basic due diligence, such as assessing the financial health of the CSP or determining how long the CSP has been in business [20]. The due diligent should not be ignored because the cloud service provider might not secure enough and they did not take responsible to the data stolen from the cloud by some hackers.

ix. Shared Technologies Issue

IaaS vendors deliver their services in a scalable way by sharing infrastructure. It is not designed to offer strong isolation properties for a multi-tenant architecture

5. CONCLUSION

Although Cloud computing can be seen as a new phenomenon which is set to revolutionise the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

REFERENCES

- F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges",
- IDC eXchange, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].
- Ashraf I 2014 An overview of service model of cloud computing Int. J. of Multidisciplinary and Current Research 2 779-783
- BalaNarayada Reddy G 2013 Cloud computing-types of cloud Retrieved from http://bigdatariding.blogspot.my/2013/10/cloud-computing-types-of-cloud.html
- Christina A A 2015 Proactive measures on account hijacking in cloud computing network Asian Journal of Computer Science and Technology 4 2 31-34

- Choubey R, Dubey R and Bhattacharjee J 2011 A survey on cloud computing security challenges and threats International Journal on Computer Science and Engineering (IJCSE) 3 3 1227-1231
- Cloud Security Alliance 2013 The notorious nine: Cloud computing top threats in 2013 Retrieved from https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cl o ud_Computing_Top_Threats_in_2013.pdf
- B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.
- S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." J Network Comput Appl doi:10.1016/j.jnca.2010.07.006. Jul., 2010.
- S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.
- M. A. Morsy, J. Grundy and Müller I. "An Analysis of the Cloud Computing Security Problem" In PROC APSEC 2010 Cloud Workshop. 2010.
- Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Mar.19, 2010]
- S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].
- A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.
- Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].
- M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." IEEE Xplore, pp 23-31, Jun. 2009.
- C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. "Business Models in the Service World." IT Professional, vol. 11, pp. 28-33, 2009.
- N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. "On Technical Security Issues in Cloud Computing" In PROC 09 IEEE International Conference on Cloud Computing, 2009 pp 110-112.
- N. Leavitt. "Is Cloud Computing Really Ready for Prime Time?" Computer, vol. 42, pp. 15-20, 2009.
- M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." in PROC IEEE ICCC, Bangalore 2009, pp. 109-116.