International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June-2018 www.irjet.net p-ISSN: 2395-0072

Challenges and Security Issues in Cloud Computing

Shashank Shashikant More[1], Dinesh J. Paliwal[2]

[1,2]*Institute of Management and Computer Studies, Thane, Maharashtra, India -400604*

Abstract: Cloud computing is Internet-based computing, whereby shared resources, software and information and also act of storing, managing and processing data online — on your own physical computers and other devices on-demand. It is an internet Based service which allows third party sharing of resources and data among devices. It is used world-wide. Cloud computing becoming most popular because it changes the way of an organization to manage their data. It provides lots of benefits such as simplicity, almost unlimited storage, least maintenance, easy utilization, backup and recovery, continuous availability, quality of service, automated software integration, document control, environmentally friendly, easy access , work from anywhere , quick deployment and cheap. Companies of all the shape and size have been adapting to this new technology. There is numerous amount of benefits from cloud computing. However, with the many advantages, come some drawbacks like security issues as well..! Cloud computing must be secure and safe and **assure** to give the privacy of the user. This paper 1St list out the architecture of cloud computing, and discuss frequently security issues of using cloud computing and some solutions to the security issues.

1. Introduction

In cloud computing the recourses are shared via internet. It provides the fast, cheap and appropriate storage and other computing services via internet. Cloud computing is a relatively new service that allow the users

To store data and access services over Internet rather than from the local hard drive which might be costly. It help to increase the storage capacity because users can have more than one cloud service to stored their data there is no need to own an expensive computer with a larger memory. Cloud Computing consist of various distinct types of computing services delivered remotely to clients via the Internet. The cloud computing having an ability to access resources on an incremental basis is levelling the playing field for small and medium sized organizations, providing them with necessary tools and technology to compete the marketplace. The cloud computing system is like your virtual computer that is a virtual location of your resources. The resources can be accessed those are placed on a cloud as on their real system resources. The user can install applications, store data etc. and can access through internet anywhere. The user do not need to buy or install any hardware to upgrade his machine. They can do it via internet. Researchers are gaining interest as there are still numerous unresolved issues which need to be addressed before large scale exploitation take place. This paper discusses the state of the art of cloud computing domain focuses on the issues and challenges and the current practices. This paper is organized as follows: Section 2 explores the related work; Section 3 describes the security issues and challenges of the current issues in cloud computing studies, Section 4 explains the solutions and practices utilize in overcoming the issues; and finally Section 5 presents the conclusion and future works of this study.

2. Related Works

The architecture of cloud composed of several service models and deployment models

2.1. Service Model:

i. Software as a service (SaaS)

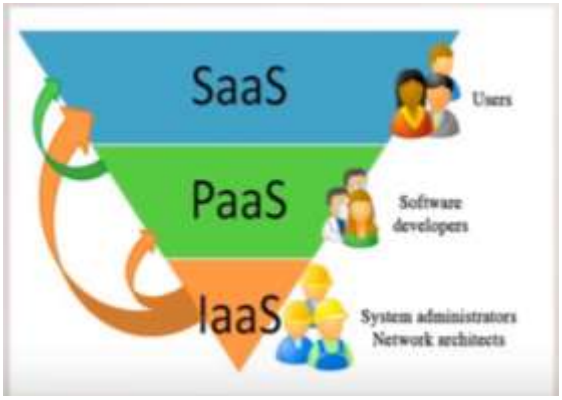
It is the top layer of cloud service model. The cloud service provider developed and hosts the software or application on the cloud infrastructure allowing the users to use it with various devices by using the thin client interface such as web browser. However the underlying cloud infrastructure, network, servers, operating systems or even individual application capabilities is not manageable by the users 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 cloud service.

ii. Platform as a service (PaaS)

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. 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.

iii. Infrastructure as a Service (IaaS)

IAAS is "Infrastructure As A Service". Here you are provided the physical Infrastructure (server, storage, Network, etc.)by vendor which you can access over the internet and use to install your software, build or deploy your application. It allow the user rent based processing, storage and other computing resources.



I. Services Model (YouTube: Thapa Technical)

3. Security Issues and Challenges

There are numerous security issues and challenges in cloud computing because it encompasses many technologies such as networks, databases, operating system, virtualization, resource scheduling, transaction management, concurrent control and memory management [1]. This is very important because the cloud service provider must ensure that the users is not facing any serious problem like data loss and data theft which may cause a great loss depending on the sensitivity of the data stored in cloud. A malicious user may pretend to be the legitimate users and infecting the cloud. There are a lot of security issues to be discussed:

3.1. Security issues

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.

3.2. Privacy issues

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. 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. [2] 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.

3.3. Application issues

Monitoring and maintenance should be done by the cloud service provider frequently to ensure that the cloud is secure and not infected by the malicious code that have been uploaded to the cloud by the hackers or attackers with the purpose of stealing sensitive information or even damaging the information of certain users.

3.4. Threats issues

i. Data Breaches :

Data stored to the cloud might be important and sensitive. And may be stoled by the unauthorized users and that might poses some level of danger to the users under attack. It is the threat the cloud computing because attackers can easily access to the data of the users which is stored in the cloud. The cloud stored a pool of confidential information of many users. The cloud service users should also ensure the quality, reliability and performance of the cloud service providers through Service Level Agreements (SLAs) negotiated between providers and users [3]. Therefore, this is the worst problem that the cloud computing service faces.

ii. 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, or natural disaster like earthquakes and fire. 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.

iii. 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 For example, the hackers might manipulate the data, provide false information and eavesdropping on transactions using the stolen account. Login with native APIs are not used so that anyone can register as a cloud service user so there are many chances of account being hijacked [4].

iv. 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 authentication and access control to the encryption and activity monitoring should be well executed to protect malicious attacks. For example, [5] propose two stage access control mechanism using the Role Based Access Control Model (RBAC) in order to provide a strong API mechanism.

v. 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.

vi. 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 reveals that password and other confidential data can be easily obtained by malicious insiders of cloud service providers. Studies by 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).

vii. 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 the International

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. 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. Insider Threats:

The employee is trust-worthy but the insider has access to servers and data owned by the victim organization. An unprotected file containing encrypted password information was found on one of these servers. The insider apply brute-force attack and access the data belonging to the victim organization's customers, and downloaded millions of personal records.

x. Spectre and Meltdown:

Meltdown is a security flaw that could allow hackers to bypass the hardware barrier between application run by users and the computers core memory which is normally highly protected. Spectre is slightly differnet.It potentially allows hackers to trick otherwise error-free applications into giving up secret information [36]

xi. Data Leakage :

CSA indicated that data leakage is the major objective with targeted attacks, which can result from human errors, application vulnerabilities and bad security measures. It can involve any information that is not suitable for open, including personal health information, financial information, personal identifying information, business secrets and intellectual property. For different reasons, one organization's cloud-based data can have more value for some other organizations. Cloud Computing is not only the service Provider that

has data Leakage but that users take it as a prior Consideration.

4. Solution and Practices for Cloud Security Issues

The cloud computing have become more popular because many users start to realize its benefits. It allows the user to easily shrink the operation and also help to save cost. However, with the increased adoption rate of the cloud service, the security issues and risk have been increased as well In order to make cloud computing a better option to increase the user storage capacity and save their confidential information securely, there are few solutions and practice that helps.

4.1. Vulnerability shielding

The cloud service provider should improve the patch management. They should check the vulnerability of their cloud service frequently and always update and maintain the cloud to limit the possible access point and reduce the risk of attack of the cloud by the hackers. The cloud service provider might also use the Intrusion Detection System (IDS) to make sure the cloud service provided is secure and safe.

4.2. Trusted cloud service provider

The user should make sure that they find the right cloud service provider. Each cloud service provider have different approaches on data management in the cloud. Well established and experienced cloud service provider is more trust worthy and better choice. Besides, the standards and regulations of the cloud service provider is also very important. Examples of trusted clouds service providers are Amazon Web Services (AWS), IBM, Google and Microsoft. [6] gives us the comparison of cloud database so that user can get better clarity of each database and choose the appropriate database accordingly. In order to guide users in choosing the best cloud service provide, Cloudscape have been developed in studies by [7]. They claimed that the application compares the cost and performance of cloud service providers and ensure fairness, representativeness and compliance while limiting measurement cost structure.

4.3. Use cloud service wisely

The data stored in the cloud should be confidential and even the cloud service provider should not have access to those information [24]. The data stored in the cloud should be well encrypted to ensure the security of the users' information. Anyone who need access to the data in the cloud should ask for the permission of the users before doing so.

4.4. Security check events

The users should have clear contract with the cloud service provider so that the users can claim if any accidents or breaches of the sensitive data stored in the cloud. The users must have clear agreement with the cloud service provider before using the cloud services provided by that particular cloud service provider. Enough details about fulfilments of promises, break remediation and reporting contingency should be ensured by service provider.

4.5. Data storage regulations

The architecture of the cloud environment is an important aspect to ensure the security of the data stored in the cloud. The users must understand the concept of the data storage regulations which the cloud service provider follows. Cloud service provider that provide security solution compliant with regulations such as HIPAA, PCI DSS, and EU data protection laws are some of the best choice.

4.6. Facilities for recovery

Cloud service provider should take the responsibility to recover the data of the users if there is any data loss due to certain issues . Cloud service provider should make sure that they have proper backup and can retrieve and recover the confidential data of the users that might be costly. Moreover, the cloud service providers can also implement the following solutions to ensure data recovery [8]: i. Using fastest disk technology in event of disaster for replication of data in danger. ii. Changing dirty page threshold. iii. Prediction and replacement of risky devices.

4.7. Enterprise infrastructure

The user must secured the data that they want to keep in the cloud infrastructure. The cloud service provider should provide an infrastructure that give facilitates for the users to install and configure hardware components like firewalls, routers, server and proxy server.

4.8. Access control

The cloud service provider should set up the data access control with rights and the users who access the data should be verified by the cloud service provider every time. The cloud service provider must ensure that only the authorized users may have access to the data stored in cloud. The method can help to reduce the risk of the data access by the unauthorized users and thus provide a much secure environment to store sensitive

data. In addition, third party auditing can also be one of the alternatives to ensure data integrity of the storage in the cloud. The procedure for auditing should contain following properties: I. Confidentiality: Auditing protocols should keep user's data confidential against auditor. ii. Dynamic auditing: Auditing protocol should support updates of data in the cloud. iii. Batch auditing: Auditing protocol should support batch auditing for multiple users and clouds

4.9. Identification management and authentication

When the user want to access the data stored in the cloud, they must be authenticated not only by using the username and password but also the digital data. Multi-level authentication technique introduced by can also be implemented in cloud computing. The technique generates password in several levels before the user can access the cloud services. Anonymous authentication (i.e. identity of user is protected from the cloud) can also be implemented where only valid users are able to decrypt the information. Other than that, proposed scheme by can also be applied in cloud computing where they claimed that their new password authentication scheme are secured from impersonation , off-line guessing and man in the middle attack. Furthermore, leakage-resilient authentication can also be utilised in order to improve the security of the cloud services.

5. Conclusion:

Cloud computing is a model that helps to speed up and increase the flexibility of data management with reduced cost. It is undeniable that cloud computing has brings us lots of benefits and becoming more popular nowadays. Many large companies start using cloud service in their business. While the cloud computing is widely used, the security becomes a concern to everyone who use cloud services. There is a lot of security arises continuously while there are improvement as well on the security model of the cloud service provided. Despite the increasing use of the cloud service, the user should use the cloud service provided wisely in a way that always ensure good security practices so that this technology have the potential to bring the information technology to the next level. Cloud computing might help us to separate he software from the hardware as more technologies are used as service using cloud and software might have a highly abstract space with the computer hardware. It is expected that this paper provides some basis or foundation in regards to issues and challenges in cloud computing.

6. References :

[1] Doelitzscher F, Sulistio A, Reich C, Kuijs H and Wolf D 2011 Private cloud for collaboration and e-Learning services: from IaaS to SaaS J. Computing-Cloud Computing 91 1 23-42

[2] Jain S, Kumar R, Kumawat S and Jangir S K 2014 An analysis of security and privacy issues,(COMPUTATIA-IV) 1-7

[3] Khoshkholghi M A, Abdullah A, Latip R, Subramaniam S and Othman M 2014 Disaster Recovery in Cloud Computing: A Survey Computer and Information Science 7 4 39-54

[4] Kill A 2013 Cloud computing risk: Due diligence and insurance Retrieved from http://www.metrocorpcounsel.com/articles/17928/cloud-computing-risks-due-diligence-andinsurance

[5] King N J and Raja V T 2012 Protecting the privacy and security of sensitive customer data in the cloud Computer law & Security Review 28 308-319

[6] Ramanathan S, Goel S and Alagumalai S 2011 Comparison of cloud database: Amazon's SimpleDB and Google's Bigtable International Journal of Computer Science Issues 8 6 2 243-246.

[7] Rocha F and Correia M 2011 Lucy in the sky without diamonds: Stealing confidential data in the cloud Proc. of the 1st Int. Workshop on Dependability of Clouds Data Centers and Virtual Computing Environments (DCDV) 1-6

[8] Mujinga M. 2013 Privacy and legal issus in cloud computing SMME position in South Africa Proc. Of the 11th Autralian Information Security Management Conf. 49-59

[9] Sen J 2013 Security and privacy issues in cloud computing Retrieved from arxiv.org/pdf/1303.4814
[9]Y Z An, Z F Zaaba & N F Samsudin