iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2017 **Issue:** onferende **Month of publication:** September 15, 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

Review Paper on Cloud Computing Security Issues and its Solution

Ajay S. Pawar[1], Prof. Pranjali Wankhede[2]
[1]*Student, Information Technology, Vishwatmak Om Gurudev College of Engineering, Thane [M.S.], India*
[2]*Assistant Professor, Computer Engineering, Vishwatmak Om Gurudev College of Engineering, Thane [M.S.], India*

Abstract: During the last two decades, the use of internet has been changing every domain of technology. It has also led to the tremendous development and implementation of cloud computing from the last few years. But the shared nature of data in the cloud makes it prone to security attacks. Also there are other security issues which may occur when we try to save our data on cloud. There are some factors needs to be considered at the time of choosing our cloud service provider. To prevent our confidential and important data there are some security techniques which are described in this paper.
Authentication is one such technique which plays a major role in Cloud Computing security. The various possible security attacks on the Cloud Service Providers (CSP) are prevented by applying different authentication mechanisms, which verifies a user's identity when a user demands services from cloud servers. There are multiple authentication technologies for verifying the identity of a user before granting access to resources. In this research work, different security issues and possible challenges possible authentication techniques are discussed. It is observed that biometric techniques are proving very helpful in implementing multi-factor authentication.

I. INTRODUCTION

Clouds provide an infrastructure for easily usable, scalable, virtually accessible and adjustable IT resources that need not be owned by an entity but can be delivered as a service over the Internet. The cloud concept eliminates the need to install and run middle ware and applications on users own computer by providing Infrastructure, Platform and Services to users, thus easing the tasks of software and hardware maintenance and support. [1]Cloud computing is a type of computing that mainly depends on resource sharing instead of handling applications by local servers or individual devices. Using the Internet enabled devices, cloud computing permit the function of application software. [2]In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users.

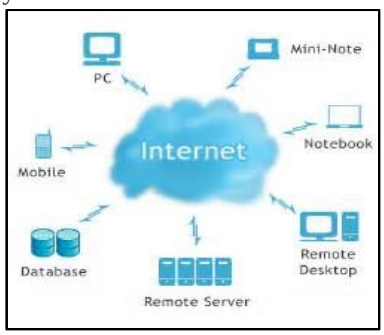


Fig.1 Cloud Computing

Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. The study represented in this paper is considered with a view to discuss and identify the approach to cloud computing as well as the security issues and concerns that must be included in the deployment towards a cloud based infrastructure. Cloud computing is a relatively new service that allow the users to store and access computing resources and data 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 and thus reduce the cost because there is no need to own an expensive computer with a larger memory.

A. Security Issues and Challenges in Cloud

[3]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. 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.

Fig.2 Cloud Security

1) [1] Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success. The security challenges for cloud computing approach are somewhat dynamic and vast.

2) Data storage is a crucial factor in cloud computing security.

3) Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated.

4) Trust is another problem which raises security concerns to use cloud service. The reason behind it is directly related to the credibility and authenticity of the cloud service providers. Trust establishment might become the key to establish a successful cloud computing environment.

5) Trust in cloud might be dependent on a number of factors among which some are automation management, human factors, processes and policies. Trust in cloud is not a technical security issue, but it is the most influential soft factor that is driven by security issues inherent in cloud computing to a great extent.

6) [4]All kinds of attacks that are applicable to a computer network and the data in transit equally applies to cloud based services – some threats in this category are man-in-the-middle attack, phishing, eavesdropping, sniffing and other similar attacks. DDoS (Distributed Denial of Service). The well-known DDoS attack can be a potential problem for cloud computing, though not with any exception of having no option to mitigate this.

7) However, it is important to distinguish between risk and security concerns in this regard. For example, vendor lock-in might be considered as one of the possible risks in cloud based services which do not essentially have to be related to security aspects. On the contrary, using specific type of operating system (e.g. open- source vs. proprietary) might pose security threat and concerns which, of course, is a security risk.

8) Data segregation and session hijacking are two potential and unavoidable security threats for cloud users. [5]One of the challenges for cloud computing is in its level of abstraction as well as dynamism in scalability which results in poorly defined security or infrastructural boundary.

9) Other examples of business risks of cloud computing could be licensing issues, service unavailability, provider's business discontinuity that do not fall within the security concerns from a technical viewpoint.

10) [5]Allocation of responsibilities among the parties involved in a cloud computing infrastructure might result in experiencing inconsistency which might eventually lead to a situation with security vulnerabilities. Like any other network scenario, the provision of insider-attack remains as a valid threat for cloud computing.

As cloud computing normally means using public networks and subsequently putting the transmitting data exposed to the world, cyber-attacks in any form are anticipated for cloud computing. The existing contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker.

[4]Intrusion detection is the most important role in seamless network monitoring to reduce security risks. If the contemporary IDSs (Intrusion detection Systems) are inefficient, the resultant consequence might be undetected security breach for cloud environment.
The facets from which the security threat might be introduced into a cloud environment are numerous ranging from database, virtual servers, and network to operating systems, load balancing, memory management and concurrency control.
Data loss and various botnets can come into action to breach security of cloud servers. Besides, multi-tenancy model is also an aspect that needs to be given attention when it comes to security.

B. Other factors needs to be considered in cloud computing are:

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. [2]Data theft is a very common issue 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.
2) *Privacy issues:* [2]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. [5]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 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) *Application issues:* Monitoring and maintenance should be done by 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.
4) *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).

Top threat that can cause serious problems in cloud computing are mentioned below.

a) *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. [6]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. The cloud stored a pool of confidential information of many users. [7]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. Therefore, data breaches are the worst problem that the cloud computing service faces.
b) *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. 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.
c) *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. 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.
d) *Insecure APIs:* Software Interface for the users to interact with the cloud services is also crucial to ensure the security of the cloud model. [8]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, propose two stage access control mechanism using the Role Based Access Control Model (RBAC) in order to provide a strong API mechanism.
e) *Denial of Service (DoS):* [8]Hacker uses 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. 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.
f) *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 has 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 reveal that password and other confidential data can be easily obtained by malicious insiders of cloud service providers. [9]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).

g) *Insufficient details about fulfilments of promises:* The users should ensure that the cloud service provider give enough details about fulfilments of promises, break remediation and reporting contingency. 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.

h) *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.

C. Solution Over 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 standards need to be maintained. They are given below as:

1) Vulnerability Shielding: [10]All the problem starts with the user by using patch software's and without any data protection software's i.e. antivirus. As a result there may be chances of loopholes which may leads to unauthorised third party access of system. Hence they should check the vulnerability of their cloud service frequently. [11]Updating and maintaining 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.

2) Trusted cloud service provider: The user should make sure that they find the right cloud service provider. Each cloud service provider has different approaches on data management in the cloud. Hence experienced cloud service provider is more trust worthy and better choice. Besides, the standards and regulations of the cloud service provider are also very important.

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. If it is then there is loss of confidentiality of data. The data stored in the cloud should be well encrypted to ensure the security of the users' information. Anyone who needs access to the data in the cloud should ask for the permission of the users and proper validation of the service user should do before doing so.

4) Security check events: The users must have clear agreement with the cloud service provider before using the cloud services provided by that particular cloud service provider. [12]The users should ensure that the cloud service provider give enough details about fulfilments of promises, break remediation and promises given by service provider. 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.

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.

6) Facilities for recovery: 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. [11]Cloud service provider should take the responsibility to recover the data of the users if there is any data loss due to certain issues. Moreover, the cloud service providers can also implement the following solutions to ensure data recovery: Using fastest disk technology in event of disaster for replication of data in danger. Changing dirty page threshold. Prediction and replacement of risky devices.

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

8) Access control: The cloud service provider should maintain verification of the authorised user before giving access to the confidential data at every time. So for that they should maintain proper validation management set up. [13]The data access control with rights and the users who access the data should be verified by the cloud service provider every time. 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, [13] third party auditing can also be one of the alternatives to ensure data integrity of the storage in the cloud.

However, the auditing procedure should have the following properties:

a) *Confidentiality*: Auditing protocols should keep user's data confidential against auditor.

b) *Dynamic auditing:* Auditing protocol should support updates of data in the cloud.

c) *Batch auditing:* Auditing protocol should support batch auditing for multiple users and clouds. [13] Identification management and authentication when the user wants 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.

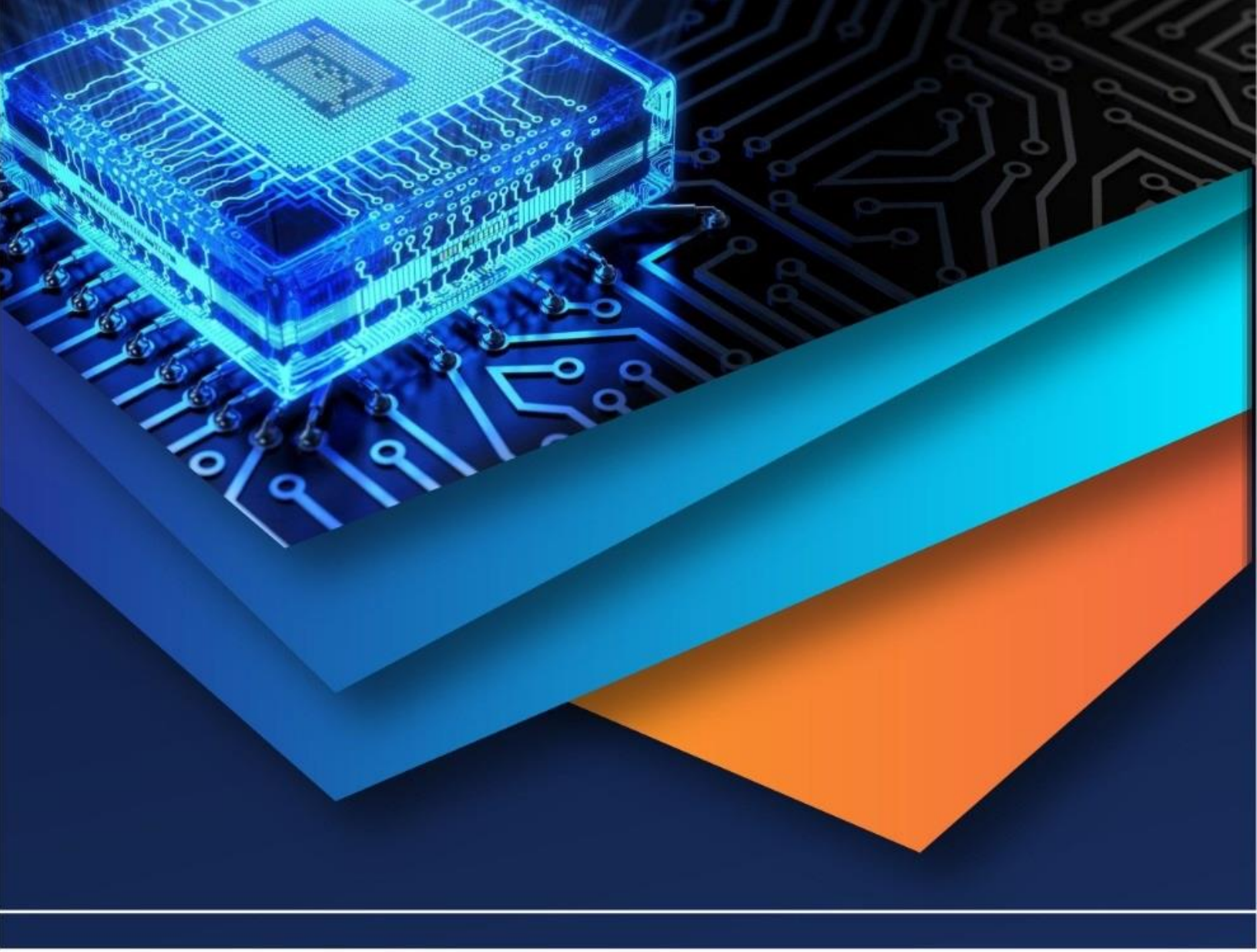
II. CONCLUSION

The benefits of use of cloud computing are clear, so it is important to develop the models, mechanisms and tools to provide the proper security of cloud implementations. The presented data provides knowledge of threats and risks in security of cloud computing, both from the point of view of cloud provider and from customer point of view. The general
awareness for security of clouds and the outline of issues related to proposed solution for cloud security. In summary, cloud computing has some advantages and disadvantages. When considering using this technology users should be aware of both. Cloud computing is cost effective, its providers offer unlimited storage capacity, much easier backup and recovery, automatic software integration, easy access to information and quick deployment. However, apart from potential technical issues, the main concern when using cloud computing is security. Clouds like anything else connected to Internet can be a target for hackers and therefore it needs to be protected. The bigger the clouds are, the bigger the risks and responsibilities are.

In addition to security, multi-level authentication technique 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.

REFERENCES

[1] Kuyoro S. O., Ibikunle F. & Awodele O. International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011 247 Cloud Computing Security Issues and Challenges.
[2] Cloud computing and security issues in the Cloud by Monjur Ahmed1 and Mohammad Ashraf Hossain2.
[3] Solutions of Cloud Computing Security Issues by Jahangeer Qadiree [1], Mohd Ilyas aqbool [2].
[4] Security Issues and their Solution in Cloud Computing by Prince Jain
[5] Laudon Kenneth C, "Management Information Systems: Managing the Digital Firm", 11th edition, Pearson Education India, 2010.
[6] www.mckinsey.com/insights/business_ technology/where_it_infrastructure_nd_business_strategy_meet.
[7] Won Kim, "Cloud Computing: Today and Tomorrow", Sungkyunkwan University, Suwon, S. Korea.http://www.jot.fm/es/issue_2009_01/column4/
[8] Pranab Kumar Das Gupta et al., "Cloud Computing-Based Projects Using Distributed Architecture", PHI Learning Pvt. Ltd., 2013.
[9] http://smallbusiness.chron.com/ description-effect-cloud-computingtraditional-infrastructure- 69534.html
[10] S Subashini, V Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, pp. 1-11, Jan 2011, Elsevier Ltd.
[11] Qi Zhang, Lu Cheng, and Raouf Boutaba, "Cloud Computing: state-of-the-art and research challenges", Journal(Springer) of Internet Services and Applications, vol.1, issue 1, pp.7-18, May 2010.
[12] Nabil Sultan, "Cloud Computing for education: A new dawn?" International Journal of Information Management, Elsevier Limited 2009.
[13] www.incapsula.com/cloud



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY