IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CLOUD COMPUTING SECURITY: A REVIEW

Shailja Kaushik

Assistant Professor

Department of Computer Applications
CGC, Landan, Mohali ,Punjab, India

Abstract— The process of using a network to store, manage, and process data, of remote servers hosted on the Internet to instead of a local server or a personal computer. With Cloud Computing we can construct our application dynamically according to our requirements. It provides us online data storage & other tools required for our applications to be used. We only need an Internet connection for accessing different types of resources and services available on the cloud. This paper will give a review about different security aspects of Clouds that provides virtual hardware and software to its user. In this review we will discuss the security of data. By using cryptographic encryption algorithms CSP can provide a level of privacy and security to the cloud users. Any user can access the data from the cloud servers through decryption by following query.

Index Terms— **Cloud Computing, Cloud Storage, Cloud Security, Cloud Service Provider(CSP)**

I. INTRODUCTION

Cloud is a form of Network which is present at remote location which can be public or private. Almost all types of applications (Email, Video Conferencing, game etc.) execute in the cloud. Cloud Computing [1] provides the facility to access any kind of information as per requirement of user. The cloud computing provides different services to their clients named as front end and back end that provides such services to the clients [2].

The basic concepts of back end (Cloud) and front end (clients) and cloud infrastructure is very simple to understand. Cloud Computing provides multiple features to its users. Some popular features provided by cloud computing are explained below to understand that what we are getting from clouds. Most of the email services which are web based like Gmail and Hotmail deliver a cloud computing service. If any user want to access his email then he only need an internet connection and a web service regardless of what kind of hardware is on that particular computer. The emails are hosted on Google's and Microsoft's servers, rather than being stored locally on the client computer of user. Now a day's many other services are present like twitter , Skype, media services like YouTube which is an example of cloud services.

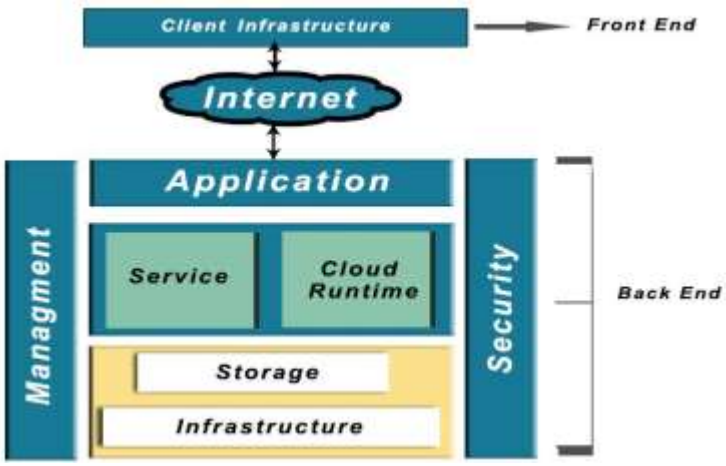


Figure-1

User need not to install any specific software to access the cloud application on his computer. Users only need to connect with internet and authenticate them on the specific cloud. Any type of user who is having authority, can access applications provided on the cloud. Using **Platform as a Service model** [3] the Cloud environment provides online application and software development. Cloud computing provides a platform independent access to the cloud resources where ever possible. The operating cost of Cloud Computing is not too much high so that many users can access it easily. Each server on the cloud provides reliable & fast services to their clients.

II. Cloud Computing Features

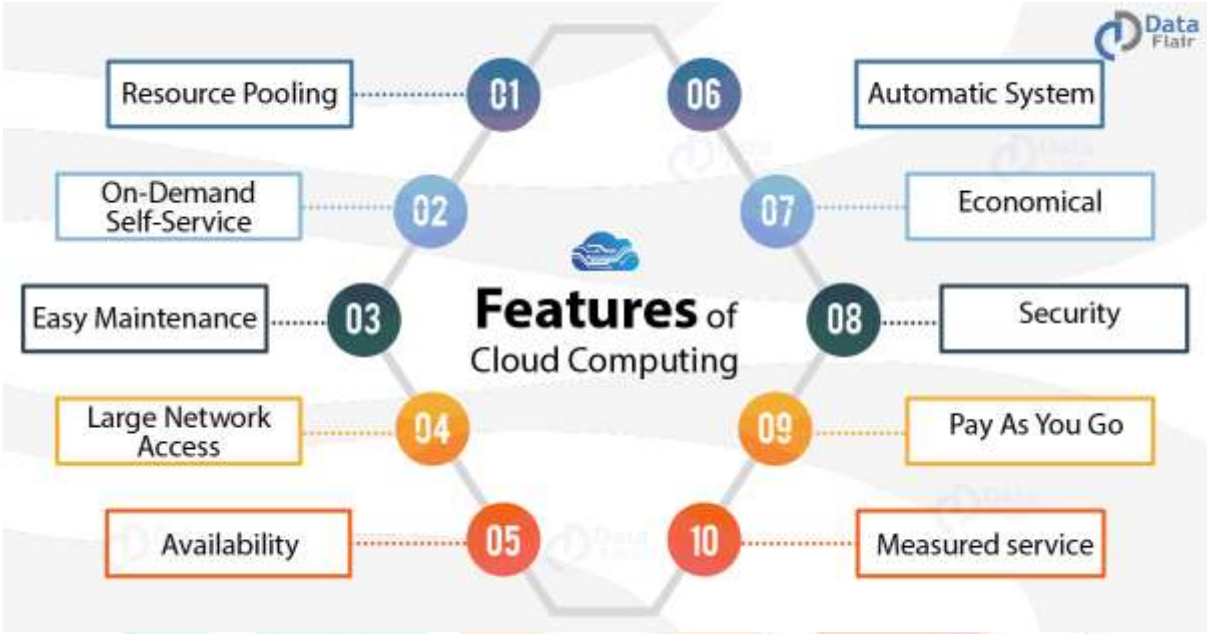


Fig. 2: Features of Cloud Computing

1. **Resource Pooling**-It is the concept of pooling resources to serve multiple clients with different physical and virtual resources dynamically assigned according to user requirement.

2. **On-demand self-service**- It refers to the service that enables the access of cloud resources on demand whenever they are required by the user.

3. **Easy maintenance**- maintenance is very easy in cloud computing.

4. **Large Network Access**- In cloud computing, it can access large networks for providing services.

5. **Availability**- Cloud computing is easily available to us without any hassle.

6. **Automatic System-** Cloud computing can be operated automatically.

7. **Economical**- Cloud computing is economical, user can choose according to his requirement.

8. **Security**- Security is also provided in cloud computing.

9. **Pay as you go-** Cloud computing also pays you as you go to clouds for providing services.

10. **Measured Service**- cloud provider measures the provision of services for various reasons, including billing, effective use of resources, or overall predictive planning so that can better understand the use of resources by the users.

III. LITERATURE REVIEW

In the past several other works are performed for the cloud data security. The literature reviews of some of these works are explained below:

In 2009, Mohammed Abdelhamid [3] proposed multiple techniques based on RSA algorithm to enhance users' privacy. "The main purpose of author is to authorize access to remotely-stored data to the users".

In 2010, S Subashini and V Kavitha [4] proposed a dynamic framework of security by different methods and techniques, Different part provides different types of security.

In 2010, M. Ahmed et al. [5] described the accuracy of various security issues related to clients and cloud resources.

In 2011, V. Krishna Reddy and Dr. L. S. S. Reddy [6] proposed the architecture of different level of cloud security. Their main aim to secure the cloud resources and client's data that is available on cloud server.

In 2011, Syam Kumar P and Subramanian R [7] proposed Elliptical Curvlet Cloud and sobel sequence for security of client data and cloud resources.

In 2012, Abbas Amini [8] proposed secure storage system for cloud computing. In their paper they uses algorithm for maintaining of accuracy of data as well as to enhance securityand for this they had used RSA Algorithm.

In 2013, Sajjad Hashemi [9] proposed different security challenges for cloud data storage.

In 2014, SwarnalataBollavarapu and Bharat Gupta [10] proposed cloud computing data storage system security for client's data. "This system uses different algorithms such as RSA, RC4 and ECC for encryption & decryption techniques".

In 2015 R. Velumadhava Rao, K. Selvamani [11] identify various Data Security Challenges and its Solutions in Cloud Computing. the main purpose of this practical examination to enhance security of data so that can maintain integrity.

In 2015, Dr. Salim Ali Abbas, Amal Abdul BaqiMaryoosh [12] provided an effective, flexible and secure method to impart security of clients' data and cloud resources.

In 2016 AL-Museelem Waleed, Li Chunlin [13] provided assessment how the lack of security is affecting user's data and cloud resources. UEC (Ubuntu Enterprise Cloud) is used in this to solve problem of secrecy of authenticity.

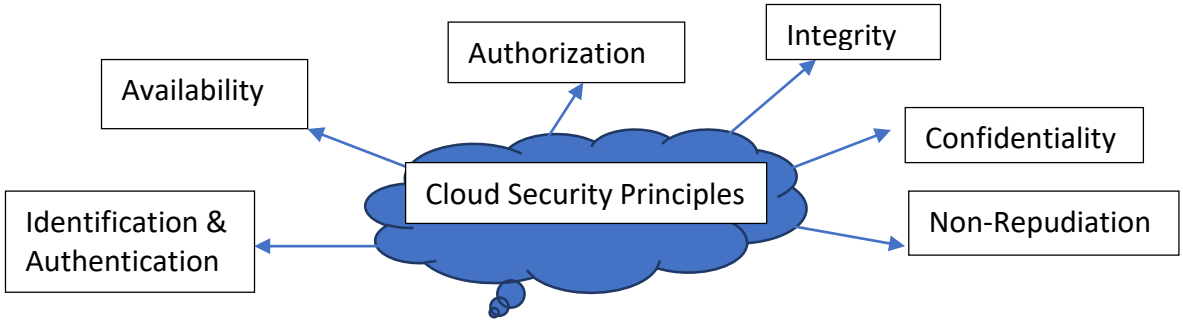
IV. CLOUD SECURITY PRINCIPLES

A cloud computing security principle determines the rules and regulations for applying security of cloud data. Six cloud computing principles defined by Ramgovind, Eloff, & Smith are explained below [15]:

1. Authorization: Authorization preserves referential integrity in cloud environment. With this rule only authorized person can access the cloud resources. All the unauthorized persons are not getting permission for accessing cloud services and resources.

2. Integrity: The integrity maintains the correctness of information stored on cloud servers. It follows ACID (Atomicity, Consistency, Isolation and Durability) property which maintains the integrity of cloud data.

3 Confidentiality: Confidentiality is a core requirement of many organizations that may be located across several distributed databases. Confidentiality is a must when we are working in a public cloud because there are so many chances that can affect integrity of data.



4. **Non-repudiation:** With this principle security of cloud data is maintained by some Security protocols and token provision for transmission of data on cloud server to client and vice versa. To maintain non-repudiation different concepts are applied such as digital signatures, confirmation acknowledgement etc.

5. **Availability:** Availability is another cloud security principle of cloud vender. We must choose cloud vender among public, private, or hybrid cloud vendors according to facility and security requirements of data.

6. **Identification & Authentication:** With this security principle we must identify the client making requests and their access privileges. If any client is not assigned to any particular service then he is not allowed to access for that service. The client authentication by username and password are also validated before accessing to any cloud service.

V. KEY SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing includes different platforms applications, infrastructure segments in it. The given below are the various security issues in a cloud computing environment.

- Access to Servers & Applications
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

VI. RISK AND SECURITY CONCERN

The general aim of security is to provide user insurance that the data is free from any kind of danger. Using this general objective a secure system guards any kind of resources from unauthorized persons[14]. Therefore to attain the proper level of security, multi-level security mechanism must be implemented in an organization to protect its assets, resources and clients' data. According to Whitman [14] different security levels that an organization must have are explained below [19].

1. **Personnel Security:** With personnel security an organization appoint authorized individual or group of individuals for accessing and allocating all the organization resources and data[17].

2 **Eavesdropping:** An unauthorized user can access the data because of interception in network traffic, it may result in failure of confidentiality. The Eavesdropper listens the private conversation of others secretly. This attack may done over email, instant messaging, etc[18]

2. **Information Security:** With information security an organization can safeguard and protect the confidentiality and correctness (integrity) and assets information for processing and storage[18].

3. **Physical Security:** With this security an organization can protect its physical assets and other essential properties from unauthorized access and misuse.

4. **Network Level Security:** With network security an organization protects its networking components & connections. It also protects organization contents that are transferred through networks.

5. **Operations Security:** With the help of operational security , an organization protects the information of all the operations and transactions performed regularly.

6. **Communications Security:** With communication security , an organization protects various contents, communications media and their technologies from unauthorized access.

All the above security levels are integrated in an organization to protect its storage, data and resources from unauthorized users.

VII. CONCLUSION

Cloud refers to any form of Network which is present at remote distance location. Cloud Computing provides us facility to access any kind of information according to the requirement o user whenever he wants to access. The advancement of cloud computing is changing the need of information technology . One of the main challenges related to cloud computing is named as data security of multiple clients. This paper provided review of different security aspects and issues of cloud data storage. This Review paper give an idea about the problems that can be occur in a cloud computing system at different security issues. In this review paper we have discuss the security aspect of cloud and make the problem formulation of security issues to be handled by research community.

REFERENCES

[1] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, "Cloud Computing, A Practical approach" [2] B. Hayes, "Cloud Computing," Commun. ACM, vol. 51, no. 7, pp. 9–11, Jul. 2008.
[2] ShankarNayakBhukya, Dr.SureshPabboju ,Dr. K Venkatesh Sharma,"Data Security in Cloud Computing and Outsourced Databases", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016 978-1-4673- 9939-5/16/$31.00 ©2016 IEEE.
[3] Mohamed Abdelhamid, PhD thesis, "Privacy-preserving Personal Information Management", School of Computer Science, McGill University, Montreal, August 2009.
[4] S Subashini, V Kavitha, "A survey on security issues in service delivery models of cloud computing", Network and Computer Applications, Elsevier, Vol. 34, pp. 1-11, 2010.
[5] Mahbub Ahmed, Yang Xiang, Shawkat Ali, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp.723-730, 2010.
[6] V. Krishna Reddy, Dr. L. S. S. Reddy, "Security Architecture of Cloud Computing", International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.
[7]. Syam Kumar P and Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.
[8] Abbas Amini, MSc thesis, "Secure Storage in Cloud Computing", Department of Informatics and Mathematical Modelling (IMM), the Technical University of Denmark, May 2012.
[9] Sajjad Hashemi, "Data Storage Security Challenges in Cloud Computing", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 2, No 4, August 2013.
[10] SwarnalataBollavarapu and Bharat Gupta, "Data Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.
[11] Dr. Salim Ali Abbas, Amal Abdul BaqiMaryoosh, "Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography", Journal of Computer Engineering, Volume 17, Issue 4, Ver. I (July – Aug. 2015), PP 48-53.
[12] Dr. Salim Ali Abbas, Amal Abdul BaqiMaryoosh, "Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography", Journal of Computer Engineering, Volume 17, Issue 4, Ver. I (July – Aug. 2015), PP 48-53.
[13] AL-Museelem Waleed, Li Chunlin, "User Privacy and Security in Cloud Computing", International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352.
[14] M. E. Whitman, Principles of information security, 4th ed. Boston, MA: Course Technology, 2012.
[15] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in Cloud computing," in Information Security for
[16[Mr.V.Biksham, Dr.D.Vasumathi," Query based computations on encrypted data through homomorphic encryption in cloud computing security", International Conference on Electrical, Electronics, and ptimization Techniques (ICEEOT) - 2016 .978-1- 4673-9939-5/16/$31.00 ©2016 IEEE
[17]Ahmed Albugmi,Madini O, Alassafi Robert Walters, Gary Wills," Data Security in Cloud Computing ,978-1-5090-1306- 7/16/$31.00 ©2016 IEEE"
[18] R. Charanya1, M.Aramudhan2, K. Mohan3, S. Nithya4"Levels of Security Issues in Cloud Computing" ISSN : 0975-4024 Vol 5 No 2 Apr-May 2013 1912 International Journal of Engineering and Technology (IJET).
[19] Mrinal KantiSarkar,Sanjay Kumar," A Framework to Ensure Data Storage Security in Cloud Computing",978-1-5090-1496-5/16/$31.00 © 2016 IEEE.
[20] https://www.calyptix.com/research-2/top-5-risks-of-cloud-computing/
[21] ShankarNayakBhukya, Dr.SureshPabboju ,Dr. K Venkatesh Sharma,"Data Security in Cloud computing and Outsourced Databases", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016 978-1-4673- 9939-5/16/$31.00 ©2016 IEEE.
[22]Z.C Nxumalo, P. Tarwireyi, M.O Adigun ," Towards Privacy with Tokenization as a Service", Department of Computer Science,University of Zululand ,Empangeni, South Africa -978-1-4799-4998-4/14/$31.00 ©2014 IEEE.
[23] http://www.thesmallbusiness.org/software/benefits- of cloud computing
[24] http://www.allthingscrm.com/cloudcomputing/understanding