ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Cloud Computing Security Issues and Encryption Techniques: A Review

Simmi Luthra

Assistant Professor, Dept. of I.T, A.C.E.T, Amritsar, Punjab, India

ABSTRACT: Cloud computing is the latest technology in the modern world. Cloud computing is the present technology in the field of distributed computing. The adoption of this technology is growing day by day because it facilitates the users to utilize the services through making use of shared pool of resources without the installation of any software. Since Cloud computing stores the data and its disseminated resources in the environment, security has become the main obstacle which is hampering the deployment of cloud environments. There are number of users used cloud to store their personal data, so that data storage security is required on the storage media. The major concern of cloud environment is security during upload the data on cloud server. But security is the critical inhibitor that are faced by cloud computing and it makes the use of cloud computing more difficult. To solve these problems, we have some encryption algorithms which provide security to the data stored on cloud. In this paper, an effort is made to review the security problems and the encryption algorithms that provide security to the cloud data.

KEYWORDS: Cloud computing, Cloud deployment models, Security issues, Encryption techniques.

I. INTRODUCTION

The term "Cloud Computing" is the computing services in Information Technology like infrastructure, platforms, or applications could be arranged and used through the internet. Cloud computing is a growing technology which has gained significant attention recently from the industry field and academia [1]. It offers services through the internet. User can deploy the services of different software by using cloud computing without buying or installing them on their own computers. It is the logical representation of the internet in the diagrams that's why is called cloud computing. Through cloud computing, users of internet can access services from a cloud as though employing a super computer. Instead of storing data in own devices they could be stored in the cloud making possible to access ubiquitous data. With software deployed in the cloud, Could also run their applications on cloud computing platforms which are more powerful, mitigating the user's burden of continual upgrade and full software installation on their local devices[2]. In cloud computing, three service models and the four deployment models are used. The service models are that which provide services to the customers on pay-per-use basis, environment for developers to build the applications and storage space to store their data. The deployment models that make the software available for use to the customers or the organizations. In the service-oriented architecture, the software as service, platform as a service and infrastructure as a service can be combined to provide the functionality of large application [2].

DOI: 10.15680/IJIRCCE.2017. 0506146

Cloud computing reduces the cost of hardware that is used by end user's. For multimedia services and applications over mobile wireless networks and Internet there is a strong demand for cloud computing, as significant amount of computation is needed for serving millions of mobile or Internet users at the same time[3]. Users process and store their multimedia application data, In[4] cloud-based multimedia computing paradigm , cloud data is stored and processed in a distributed manner, eliminating full installing on users' device or computer the media application software and thus alleviating the burden computation of user devices and saving the battery of mobile phones.

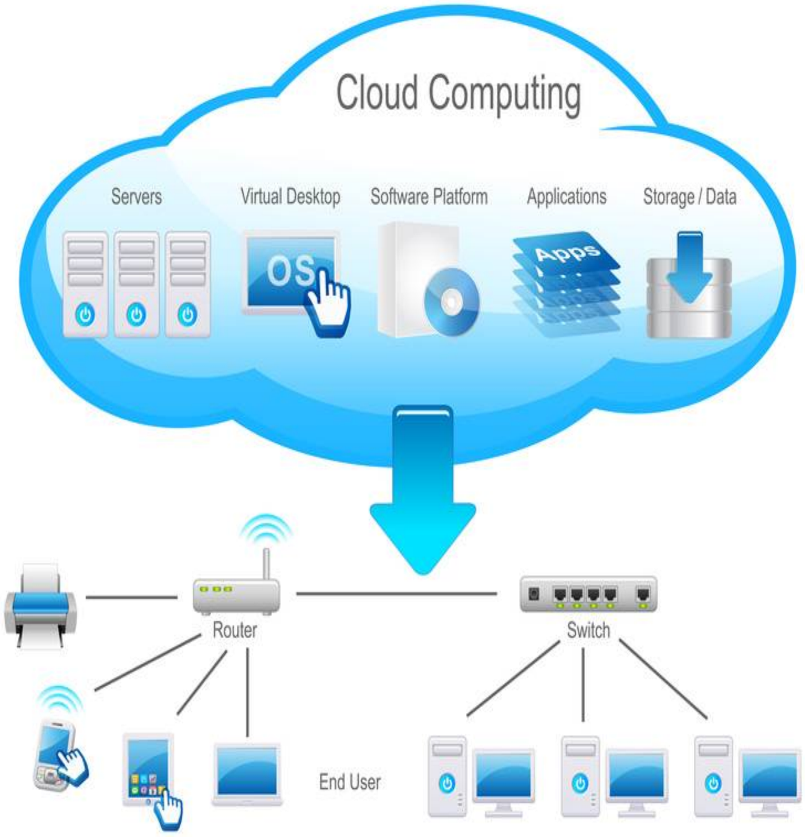

Figure 1: **Cloud computing**

II. CLOUD DEPLOYMENT MODELS

A. Public Cloud: Private cloud is a term used to donate a proprietary computing architecture provisioned services on corporate networks. Big enterprises usually used this type of cloud computing to permit their private network and information Centre administrators to effectively become in-house 'service providers' catering to customers within the corporation[6]. Cloud organization is establishing for a particular aggregation and managed by a third party under a service level agreement. Only single organization preferred to operate via corporate cloud. There are advantages (benefits) of internal cloud model. The diagram given below depicts a few of these advantages (benefits)

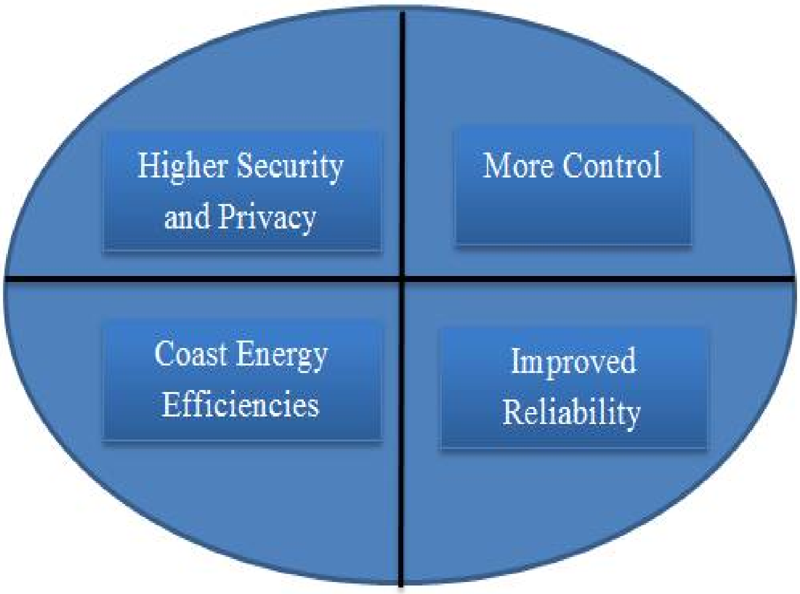

Figure 2: **Public cloud benefits**

B. Hybrid Cloud: A hybrid cloud comprises assets from both corporate and public providers will definitely become the demanded choice for enterprises [8]. The hybrid cloud is a combination of both corporate cloud and public cloud. For example, for general computing enterprise could selects to make usage of external services, and its own data Centre's comprises it own data Centres. Hybrid cloud model has number of advantages (benefits).The diagram given below reveals some of those advantages (benefits) [8].

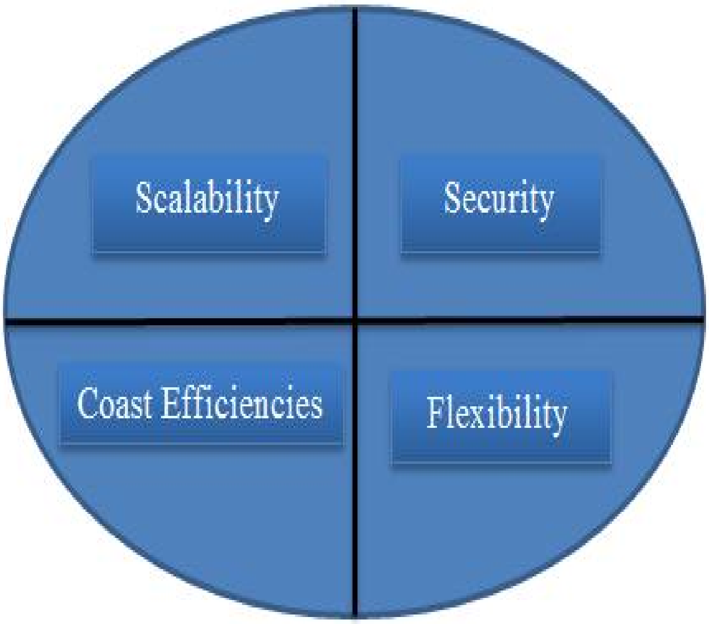

Figure 3**: Hybrid cloud benefits**

III. SECURITY ISSUES

A. Location Transparency: It is the one of the well-known work ability for cloud computing, which is a security problem at the same time, without knowing the exact location of the data storage [14].

B. Data Security: Data Security refers as a confidentiality, integrity and availability. These are the major issues for cloud vendors. Confidentiality is defined as a privacy of data. Confidentiality are designed to prevent the sensitive information from unauthorized or wrong people. In this stores the encryption key data from enterprise C, stored at encrypted format in enterprise D. that data must be secure from the employees of enterprise D. Integrity is defined as the correctness of data, there is no common policies exit for approved data exchanges[15].

C. Distributed Denial of Service: It can be a potential or serious problem for cloud computing. In cloud computing infrastructure, it is the major common attack until now and there is no option to mitigate this type of problem.

D. Regulatory Complaince: Customers are eventually accountable when the security and completeness of their own data is taken by a service provider. Traditional service providers more prone to outsource surveys and security certification. Cloud computing providers reject to endure the scrutiny as signaling so these customers can only make usage of paltry operations.

E. Data Access: This issue is mainly related to the security policies that are given to the customers or users while accessing cloud data. In typical situation, an organization can use the cloud that is provided by other provider to conducting its business processes. Each employee of a organization have considered policies to access the business data stored on cloud[17]. To avoid, disruption by the unauthorized access the security policies must be closely followed by cloud.

F. Trust Issue: Trust is also a major issue in cloud computing. Trust can be in between human to machine, machine to human, human to human, machine to human. Trust is revolving around assurance and confidence. In cloud computing, user stores their data on cloud storage because of trust on cloud. For example people use Gmail server, Yahoo server because they trust on provider.

G. Data Locations: When users use, they probably won't know exactly where their data will hosted and which location it will stored in. In fact, they might not even know what country it will be stored in. Service providers need to be asked whether they will accomplish to storing and alter data in particular arbitration, and on the basis of their customers will they make a fair accomplishment to follow local privacy requirement.

H. Data Recovery: It is defined as the process of restoring data that has been lost, corrupted or accident.

IV. ENCRYPTION TECHNIQUES

1. Server-side Encryption With this option all data is encrypted in storage by the cloud platform itself. Server-side encryption really only protects against a single threat: lost media. It is more a compliance tool than an actual security tool because the cloud administrators have the keys anyway. Server-side encryption offers no protection against cloud administrators [13].

2. Client/Agent Encryption If you don't trust the storage environment your best option is to encrypt the data before sending it up. In it we turn a shared public resource into a private one by encrypting it while retaining the keys.

3. Proxy Encryption One of the best options for business-scale use of object storage, especially public object storage, is an inline or cloud hosted proxy. There are two main topologies:

- The proxy resides on your network, and all data access runs through it for encryption and decryption.

• The proxy runs as a virtual appliance in either a public or private cloud.

V. METHODOLOGY

Security of data and trust problem has always been a primary and challenging issue in cloud computing. This section describes a methodology as shown in figure 2 to ensure security in cloud computing. The two different approaches used are as follows:-

A. Extensible Authentication Protocol-CHAP: EAP stands for Extensible Authentication Protocol. It offers a basic framework for authentication. Many different authentication protocols can be used over it. New authentication protocols can be easily added. EAP works over a secure line. A client may not support all authentication methods so EAP must support authentication method negotiation [15]. It also allows for mutual authentication by running the protocol in both directions. In our purposed model we use Challenge Handshake Authentication Protocol (CHAP) for authentication.

B. Rijndael encryption Algorithm: The Rijndael is a symmetric block cipher algorithm with key sizes ranging from 128, 192, and 256. A symmetric algorithm is one in which the cryptographic keys for encrypting plain text and decrypting cipher text are the same. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers. Stream ciphers encrypt data each digits separately and individually whereas block cipher algorithms encrypt text in blocks an pad original plain text so that the size it matches the block size. It uses the encryption of 128 bit blocks. Rijndael is an iterated block cipher, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function).

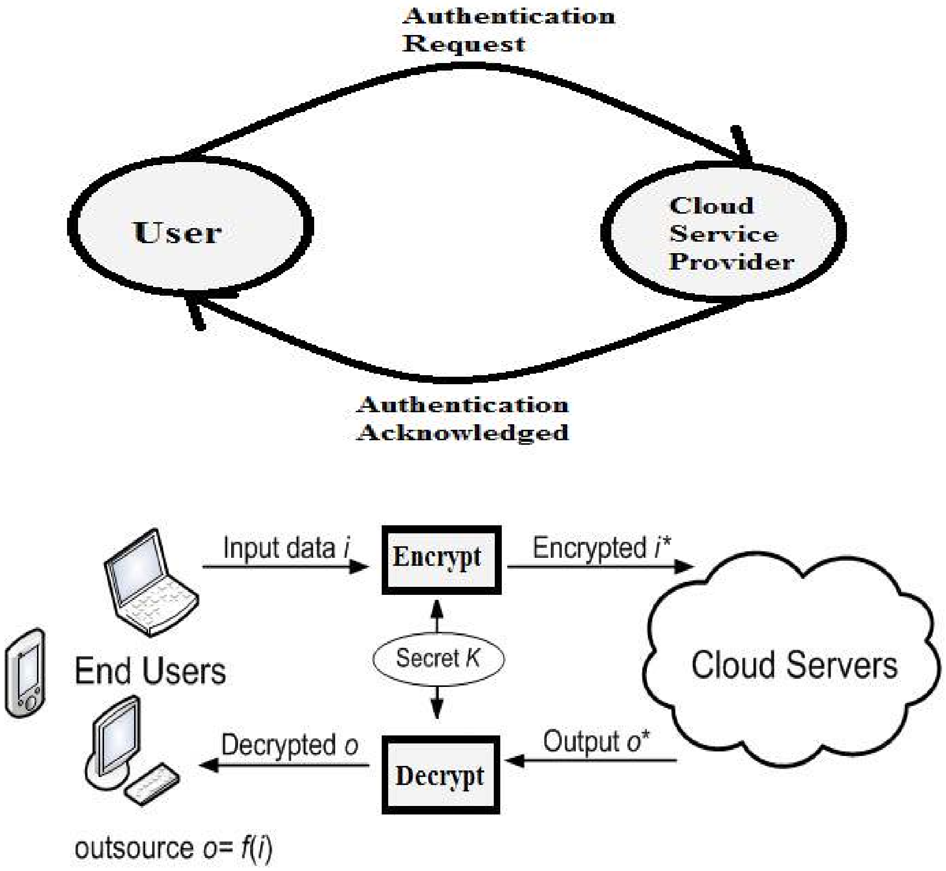

Figure 4: **Methodology**

VI. CONCLUSION

Cloud computing is relatively a new technology that provides vast benefits to the users. Cloud computing has huge visions, but the security hazards placed in cloud computing approach are directly related to the benefits that it offers. For both the businesses and the hackers or attackers, cloud computing is a great chance and profitable. Security is a inflexible requirement for cloud computing environment. We have presented the various cloud computing security issues and the solutions for this. Although cloud computing has many advantages, there are still many actual problems that need to be solved. The main problem is to maintain the privacy and the confidentiality of the data. Data confidentiality can be achieved by encrypted outsourced content before outsourcing to cloud servers and for privacy it is required that only the authorized user can access the data. Even if some intruder (Unauthorized user) gets access of the data accidentally or intentionally, he will not be able to decrypt it. In my work, I have used Rijndael Encryption algorithm to provide security to the data and EAP-CHAP for authentication purpose.

REFERENCES

1. Chandrahasan, R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam. "Research Challenges and Security Issues in Cloud Computing." International Journal of Computational Intelligence and Information Security 3.3 (2012): 42-48.
2. Parsi Kalpana, Sudha Singaraju, " Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.
3. B.R kandukuri, R.Paturi V, and A.Rakshit, "cloud security issues",2009 IEEE International Conference on Services Computing, sep. 21-25, 2009, Bangalore, India, pp. 517-520.
4. Tejas P. Bhatt, Ashish Maheta, "Security in Cloud Computing using File Encryption", International Journal of Engineering Research and Technology(IJERT), Vol. 1 Issue 9, November 2012.
5. Feng-Tse Lin, Teng-San Shih, "Cloud Computing: The Emerging Computing Technology," ICIC Express Letters Part B: Applications (ISSN: 2185-2766), v1, September 2010, pp. 33-38.
6. Kant, Dr Chander, and Yogesh Sharma. "Enhanced Security Architecture for Cloud Data Security." International Journal of Advanced Research in Computer Science and Software Engineering 3.5 (2013): 571-575.
7. Keiko et al. "An analysis of security issues for cloud computing", Journal of Internet Services and Applications 2013
8. Ren K, Wang C, Wang Q (2012), "Security challenges for the public cloud.", IEEE Internet Compute 16(1):69–73.
9. Cloud Security Alliance, "Top Threats to Cloud Computing v1.0," Prepared by the Cloud Security Alliance, March 2010, pp. 1-14.
10. Boldreva A., Chenette N., Lee Y, O'neill A. (2009), "Order-preserving Symmetric encryption", Advances in Cryptology-EUROCRYPT 2009 Springer, Berlin/Heidelberg, pp. 224-241.
11. Defending Cloud Data with Infrastructure Encryption, Version 1.0, and July 12, 2013.
12. Amit et al. "Enhancing Security in Cloud Computing Using Bi-Directional DNA Encryption Algorithm" Springer 2015.
13. Rachna et al. "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA) , Vol. 3, Issue 4
14. Dr.A.Padmapriya et al. [4] "Cloud Computing: Security Challenges & Encryption Practices", Volume 3, Issue 3, March 2013.
15. Sonali Madireddi, "Implementing Cloud Security by Encryption using Block Cipher Algorithms", International Journal of Applied Information Systems (IJAIS), Vol. 4-No. 11, December 2012.
16. Prashant Rewagad, Yogita Pawar, "Use of Digital Signature and Rijndael encryption Algorithm to Enhanced Security of data in Cloud computing Services", proceeding published in International Journal of Computer Applications (IJCA), 2012.
17. Pratiyush Guleria, Vikas Sharma,"Development and Usage of Software as a Service for a Cloud and Non-Cloud based Enviroment-An Empirical Study", International Journal of Cloud Computing and Services Sciences(IJ-CLOSER), Vol. 2, No. 1, February 2013.
18. http://en.wikipedia.org/wiki/Cloud_computing.
19. Parsi Kalpana, Sudha Singaraju, " Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 22785841, Vol 1, Issue 4, September 2012.
20. http://thegadgetsquare.com/1552/what-is-cloudcomputing/.