© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 04 , Issue : 08 | October - December 2017

ENHANCING SECURITY OF CLOUD SERVER USING CRYPTOGRAPHY: A REVIEW

Renu[1], Priyanka singla[2]
[1]Research Scholar , Department of CSA, Ch. Ranbir Singh University, Jind, renukajalk17@gmail.com
[2]Assistant Professor, Department of CSA, Ch. Ranbir Singh University, Jind, singla.priyanka198@gmail.com

ISSN : 2348-5612 © URR

Abstract: Cloud services are offering flexible & scalable services. But there is always issue of security in traditional cloud based systems. When data is transferred from centrally located server storage to different cloud the technical complexities increases. There is always risk to confidentiality & availability of data prior to selecting a cloud vendor or choosing own cloud & cloud service migration. Cloud services usually have their securityconcerns that must be addressed. In this paper, we have discussed threats to cloud service & data in case of traditional security system. We have also discussed modern security systemto secure data on cloud. Security is provided using multiple layers.

Keyword: Cloud Computing, IAAS, SAAS. AES, Security.

[1] INTRODUCTION

Cloud may be network or internet & it is something that is available at remote place[5]. It provides services over network that are public & private. They are used in wide area network, local area network or virtual private network. Several application like email & web based conferencing executes on cloud.

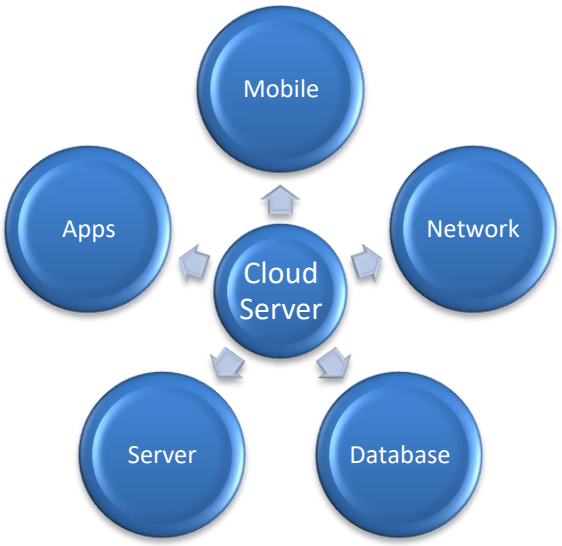

Fig 1 Cloud sever

Platform independency is offered by cloud computing because there is no need to install software on personal computer. So we can say that our business applications are mobile & collaborative due to cloud computing.

There are several services that are making cloud computing more feasible & easily accessible to users. Cloud computing is providing number of advantages but there are several risks associated with this technology.

[2] CLOUD SERVER MODEL

Type of access to cloud has been defined by Deployment model[8]. There are four types of accessibility in cloud that are public access, private access, Hybrid access & Community access.

Public Cloud

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free.Access to general public is allowed by public cloud. Due to openness public cloud is less secure[8].

Private Cloud

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally. Private clouds are considered safer& secure [18].

Community Cloud

Accessibility to a particular group is allowed by community cloud. Community cloud shares infrastructure between several organizations from a specific community with common concerns. It is managed internally or by a third-party, and hosted internally or externally [18].

Hybrid Cloud

Hybrid cloud is a composition of two or more clouds such as private, community or public which remain distinct entities. But they are bound together and offer the benefits of multiple deployment models. Hybrid cloud means the ability to connect collocation, managed and dedicated services with cloud resources.[18]

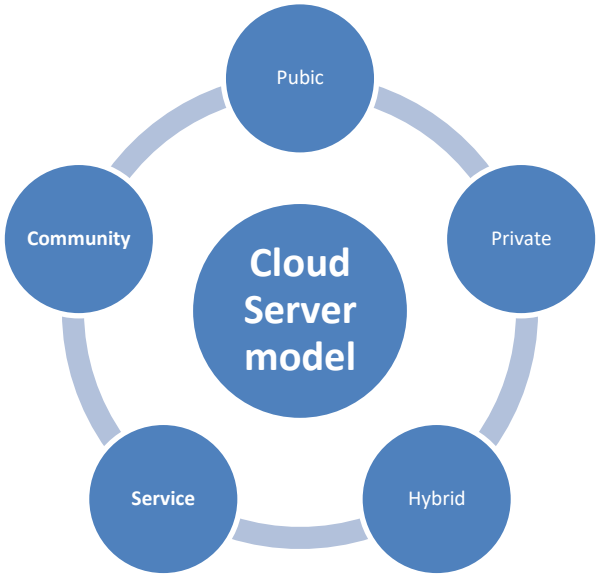

Fig 2 Cloud Server model

Service Models

There are three service models in cloud computing. First is Infrastructure as a Service, Second one is Platform as a Service & last one is Software as a Service[7].

[3] LITERATURE REVIEW

Saju Mathew (2012)Implementation of Cloud Computing in Education[1]

Author has explain main object to identify special of cloud computing which can be considered as a latest dawn to higher education & has full potential to make a revolution in field of education.

Security Threats in Cloud Computing Environments byKangchan Lee(2012)[2]

The security for Cloud Computing is emerging area for study & this paper provide security topic in terms of cloud computing based on analysis of Cloud

Security treats & TechnicalComponentsof Cloud Computing.Security Threats in Cloud Computing are:

- **Misuse of computational resources**: The hackers might misuse the computing capability that has been provided by clouds by conducting illegal activities. It increases the capability for users to customize a realistic environment that consist of virtual machines running with different operating systems.
- **Data loss**: Data loss is considered an important security risk of cloud models.

Mladen A. Vouk (2014) Cloud Computing Issues, Research & Implementations Cloud[3]

There are lot of research in distributed computing, networking and software services. It explainservice architecture, cheap informationtechnology overhead for end-user. This research also considers greatelasticity, reduced total cost of ownership, on demand services & many other things related to cloud computing.

Raj Kumar (2015) Research on Cloud Computing Security Threats using Data Transmission [4]

Computer Science & Software Engineering Cloud computing is set of resources & services offered through Internet. Cloud services model should delivered from security data centres located throughout world. Cloud computing facilitates its consumers by providing virtual resources via internet. General example of cloud services is Google apps, provided by Google & Microsoft SharePoint. The rapid growth in field of “cloud computing” also increases severe security concerns.

[4] PROBLEM STATEMENT

Third party provides data & infrastructure management in cloud computing so security of cloud is biggest concern.[3] There is a risk in providing sensitive data to cloud service provider. Any security breach could result in customer or business loss so vendors provide protection to accounts.

When data is transferred over cloud network there is always threat from crypto analyst. In order to secure the data and to disable unauthentic user to understand the data there is need of cryptography.

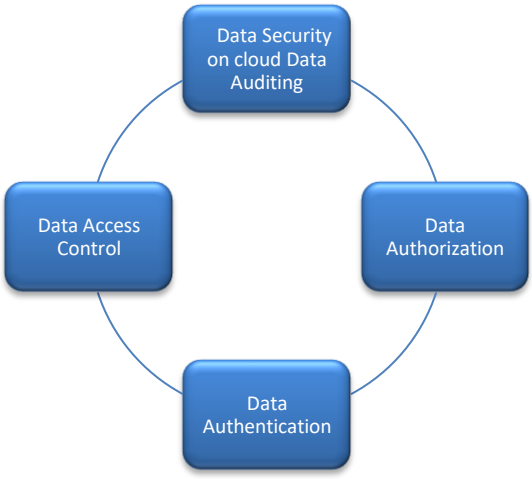

Fig 3 Data Security on cloud

Customer cannot switch from one cloud service provider to another quickly so he is dependent on cloud service provider for service. Customer management interface is usually accessible on network in case of various public cloud service providers.

Data security must be considered in cloud because data is frequently transferred over Internet [4]. The basic mechanisms to protect data over cloud are data

auditing, data access control, data authentication & data authorization.

[5] TOOLS AND TECHNOLOGY

Socket Programming

The endpoint in an inter process communications called a socket, or a network socket for disambiguation.[7] Since most communication between computers is based on the Internet Protocol, an almost equivalent term is Internet socket.

Client server Model

It is possible for two network applications to begin simultaneously. But it is not practical. Therefore, it makes sense to design communicating network applicationsto perform complementary network operations in sequence, rather than simultaneously.

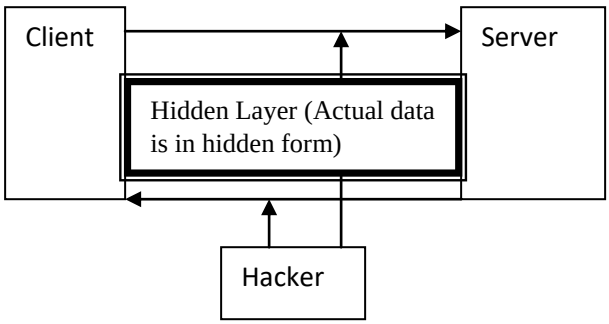

Fig 4 Client Server model

A special function issued by having distortion & picture subroutines used as password in order to save password from offline dictionary attack[7].Work is implemented in one of major used language named java.

[6] ENHANCING SECURITY IN CRYPTOGRAPHY

Modern cryptography is heavily based on mathematical theory and computer science practice [7]. Cryptographicalgorithms are designed around computational hardness assumption making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means [17].

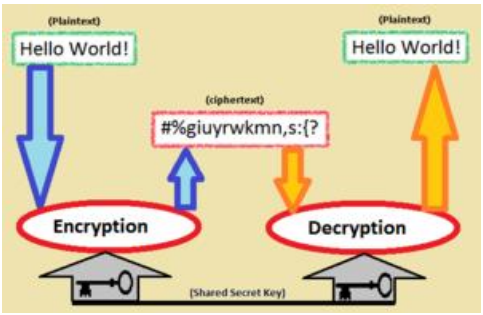

Fig 5 Encryption and Decryption of text

Encryption and Decryption of textmade for the security purposes in cloud network. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks. Cryptographyis the art of achieving security by encoding messages to make them non-readable[7].Cryptography is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography.

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 04 , Issue : 08 | October - December 2017

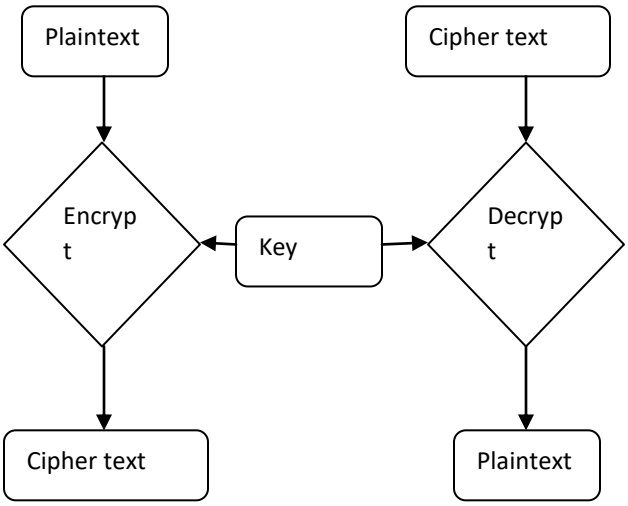

Fig 6 Key concept in cryptography

DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard is a block cipher, meaning a cryptographic key & algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt a plaintext message, DES groups it into 64-bit blocks.

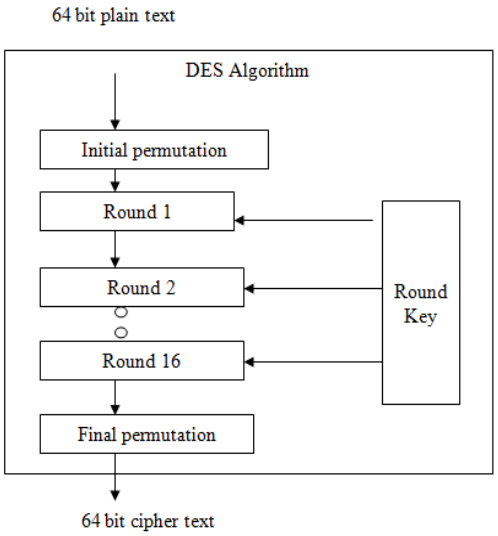

Fig 7 DES

Advanced Encryption Standard (AES) Advanced Encryption Standard is a symmetric encryption algorithm. Algorithm has been developed by two Belgian Cryptographer Joan Daemen& Vincent Rijmen.AES has been developed to be efficient in hardware as well as software. It generally allows a block length of 128 bits & key lengths of 128, 192, and 256 bits.

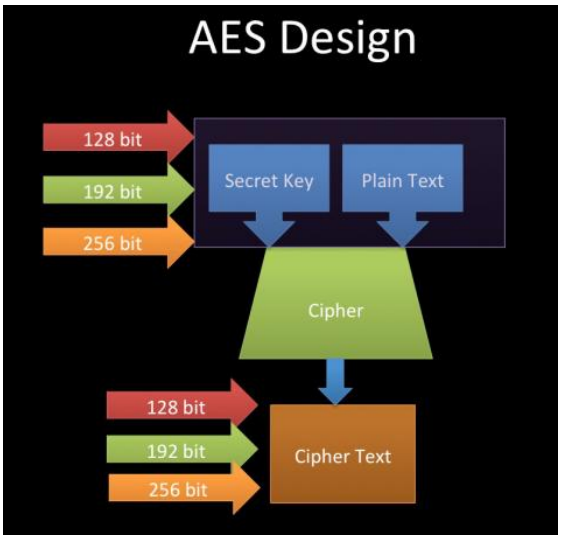

Fig 8 AES

Fig 8 AES General Structure

[7] OBJECTIVEOF RESEARCH [2]

The main objective of research is to study the loop holes of existing systems and made more efficient security system.

1. Establishment of cloud computing Environment in order to share data.
2. Study of security threats to existing cloud network.
3. Designing more secure security mechanism.
4. Make Comparative study of existing security mechanism with proposed model.
5. Investigation of limitation of existing cryptographic techniques
6. Development of application program interface using network programming to

Integrate security to cloud network by customized cryptographic techniques.

[8] CONCLUSION& FUTURE SCOPE

In modern area there is need of security for cloud based systems. However the there are several research made in this field. They have used many security mechanisms for data security. But some of them are less efficient. Many systems consume lot of time to process the data during transmission. Thus there is need of more efficient and fast security system for cloud computing.

The conclusion of this research is that there is requirement of more secure cloud computing environment.

Cloud computing relies on sharing of resources to achieve coherence & economy of scale, similar to a utility over an electricity networkAdvocates claim that cloud computing allows companies to ignore up-front infrastructure costs. This research is implementing cloud computing in order to share data and study of security threats to existing cloud network. Here we make Comparative study of existing security mechanism. We have also make investigation of limitation of cryptographic techniques. But there would issue of security due to data transfer from one cloud server storage to another cloud. This research would reduce the risk to the confidentiality and availability of data prior to selecting a cloud vendor or choosing own cloud. The security concerns of cloud services have been addressed in our research. The proposed system has wide scope and it has additional security and data transmission feature as compare to traditional.

REFERENCE

1. Saju Mathew (2012),“Implementation of Cloud Computing in Education”,International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012
2. Kangchan Lee(2012), “Security Threats in CloudComputingEnvironments”International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012
3. Mladen A. Vouk (2014),“Cloud Computing Issues, Research & Implementations Cloud”,International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014
4. Raj Kumar(2015),“Research on Cloud Computing Security Threats using Data Transmission”,International Journal of Advanced Research,Volume 5, Issue 1, January 2015
5. Peter mill & Tim grance(2011), “The NIST Definition of Cloud Computing”, National Institute of Standards & Technology, GaitherbsburgMD 20899-8930, NIST Special Publication 800-145.
6. Ellen Messmer,(2011) “New security demands arising for virtualization, cloud computing”, security-demands-arising-for-virtualization—cloud computing.html
7. .SumedhaKaushik&AnkurSinghal,(2012) “Network Security Using Cryptographic Techniques”, International Journal of Advanced Researchvolume 2, Issue 12.
8. Rouse, Margaret. "What is public cloud?". Definition from Whatis.com. Retrieved 12 October 2014.

9. Charles Miers, Fernando Redigolo& Marcos Simplicio,(2012) "A quantitative analysis of current security concerns & solutions for cloud computing", Journal of Cloud Computing: Advances, Systems & Applications electronic
10. Rabi Prasad Padhay, (2012) "An Enterprise Cloud Model for Optimizing IT Infrastructure", International Journal of Cloud Computing & Services Science (IJ-CLOSER) Vol.1,
11. Nelson Gonzalez, et. al.(2012), "A quantitative analysis of current security concerns & solutions for cloud computing", Journal of Cloud Computing: Advances, Systems & Applications electronic version of this article is complete one & could be found online
12. .CSA (2009) "Security Guidance for Critical Areas of Focus in Cloud Computing", Tech. rep., Cloud Security Alliance.
13. Rowstron& P. Druschel. Pastry (2001), "Scalable, distributed object location & routing for large-scale peer-to-peer systems",*Accepted for Middleware, 2001*, 2001.
14. Ben Y. Zhao, John Kubiatowicz, & Anthony Joseph. Tapestry(2001),"an infrastructure for fault tolerant wide-area location & routing.", April 2001.
15. Andr´ea W. Richa C. Greg Plaxton, RajmohanRajaraman(1997),"Accessing nearby copies of replicated objects in a distributed environment", In *Proceedings of ACM SPAA*, pages 311– 320, June 1997.
16. Stefan Saroiu, P. Krishna Gummadi& Steven D. Gribble(2001), "A Measurement Study of Peer-to- Peer File Sharing Systems", July 2001.
17. Ion Stoica, Robert Morris, David Karger, M. FransKaashoek, &HariBalakrishnan. Chord: A peer-to-peer lookup service for internet applications. August 2001.
18. *Peter Mell and Timothy Grance (September 2011).* The NIST Definition of Cloud Computing *(Technical report). National Institute of Standards and Technology: U.S. Department of Commerce.* Doi:10.6028/NIST.SP.800-145. *Special publication 800-145.*