International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-212 PAGE NO: 1321-1328
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

CYBER SECURITY IN CLOUD COMPUTING USING DES ALGORITHM

M.Saranya[1], Dr.T.Ramaprabha [2],
[1]M.Phil Full time research scholar, PG and Research Department Of Computer Science
[2]Professor, PG and Research Department of Computer Science.
Vivekanandha College of Arts and Sciences for Women (Autonomous)
Tiruchengode, Tamilnadu, Namakkal-637205,
ramaradha1971@gmail.com
saansaranyaa1421@gmail.com

ABSTRACT- Cloud Computing is a set of IT Services, for example network, software system, storage, hardware, software, and resources and these services are provided to a customer over a network. The IT services of Cloud Computing are delivered by third party provider who owns the infrastructure. Benefits of cloud storage are easy access means access to your knowledge anyplace, anyhow, anytime, scalability, resilience, cost efficiency and high reliability of the data. Because of these benefits each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). In this research paper, the proposed work plan is to eliminate the concerns regarding data privacy using cryptographic algorithms to enhance the security in cloud as per different perspective of cloud customers.

Keywords: Cloud Computing, Cryptographic Algorithm, Infrastructure, Internet, Security Issue.

I. INTRODUCTION

Cloud Computing is the ability to access a pool of computing resources owned and maintained by a third party via the Internet. It is not a new technology but a way of delivering computing resources based on long existing technologies such as server virtualization. The "cloud" is composed of hardware, storage, networks, interfaces, and services that provide the means through which users can access the infrastructures, computing power, applications, and services on demand which are independent of locations. Cloud computing usually involves the transfer, storage, and processing of information on the 'providers' infrastructure, which is not included in the 'customers' control policy.

It satisfies the on-demand needs of the user. It facilitates the sharable resources "as-a-service" model. For the organization, the cloud offers data centers to move their data globally. It eliminates the responsibility of local nodes for maintaining their data and also cloud supports customizable

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-212 PAGE NO: 1321-1328
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

resources on the web. Cloud Service Providers maintains computing resources and data automatically via software. Need of the user. It facilitates the sharable resources "as-a-service" model

II. CLOUD SERVICES MODELS

Cloud Infrastructure as a service (IaaS)

In this composition of implemented environment for their system a supplier must be supply a different computing resource which include loading, processing unit. Client has flexile to achieve and switches software mutilated to be implemented and vary between different applications like operating system etc.

Cloud Platform as a service (PaaS)

This software supplies client with the ability to establish and extended applications that are mainly positioned on equipment and programming languages promoted by the suppliers. In this the client has no containment over the different organization but has containment over the extended applications. Examples of this class of services include Google App Engine, Windows Azure Platform and rack space. There are different issues in PaaS such as:

- Application Delivers only Environments
- Standalone Developments Environments
- Open Platform & Open Service
- Add on Development Possibility

Cloud Software as a service (SaaS)

This software supplies the ability to usage the appliances which implemented on cloud organization. With the usage of standard interfaces like web browser or online (e-mail) client, these appliances are obtainable. SaaS appliances are obtained from different devices like mobile, workstation from anywhere at any time.

Cloud Network as a service (Naas)

Naas provides the capability to use the network services and inter-cloud network connectivity services. Improvement of possession allocation services include in view of network and computing resources. These type of services involved extensible, enhanced virtual private network. .

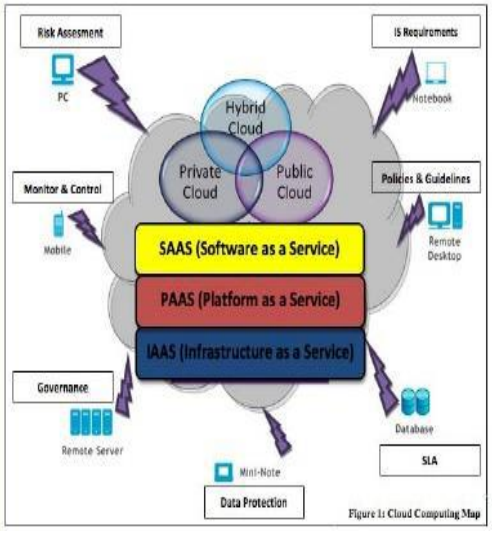


Figure 1: Cloud computing Services

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-212 PAGE NO: 1321-1328
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

III. CLOUD CHARACTERISTICS

On Demand self-service:

A cloud might individually attain computing possibilities, as per the use of different servers, network storing, as on request, without communicating with cloud provider.

Broad Network Access:

Services are delivered across the Internet within a standard mechanism and access to the services is possible through assorted customer tools.

Rapid Elasticity:

Capabilities might be elastically provisioned or rapidly released. From customers view, the provided possibilities come out to be limitless and must have the capability to purchase in any quantity at any time.

IV. SECURITY ISSUES

Storage, Backup and Recovery:

When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers. In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

Data Recovery:

It is defined as the process of restoring data that has been lost, corrupted or accident. Whenever a discussion about cloud security is taken place there will be very much to do for it.. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. There are four types of issues raise while discussing security of a cloud.

Data Issues:

Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data.

Environment. Physical location of data storage is very important and crucial. It should be transparent to user and customer. Vendor does not reveal where all the data's are stored.

Secrecy Issues:

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-212 PAGE NO: 1321-1328
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

maintaining the server so that it enable the provider to protect the customer's personal information.

CLOUD SECURITY vs CLOUD MODELS

Security is considered as one of the most critical aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven't been fully evaluated with respect to the security.

- Deployment Models and its security challenges
- Service models and its security challenges
- Network issues on Cloud
- There are some key securities challenges are
  - Authentication
  - Access Control
  - Policy Integration
  - Service Management

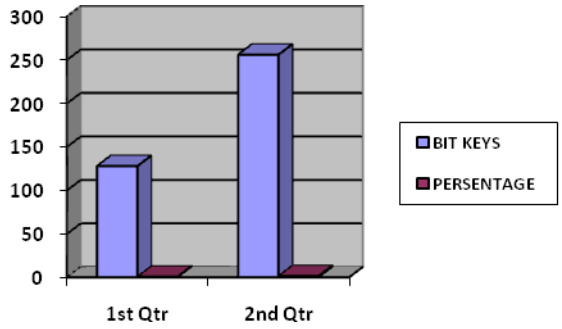
CYBER SECURITY IMPLEMENTION ON CLOUD

Data Security Model

User's data can be made secure in the cloud using encryption. But the question arises that is user's data actually encrypted when it is stored in the cloud? For example, EMC's Mozy Enterprise does encrypt user's data whereas AWS S3 does not encrypt user's data.

A performance evaluation reveals that going from 128 bits key to 192 bits key causes increase in power and time consumption by 8% and 256 bits key causes an increase of 16%. So we propose use of industry-standard high grade Advanced Encryption Standard (AES) symmetric encryption algorithm with key length of 128-bits for this purpose.

S.NO	BIT KEYS	PERSENTAGE
1	128	8%
2	256	16%



EXISTING ALGORITHMS FOR CLOUD SECURITY

In Cloud Storage any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data. In Symmetrickey encryption, only one key is used to encrypt and

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-212 PAGE NO: 1321-1328
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

decrypt the data. Another technique is known as asymmetric key encryption where two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption There are a number of existing techniques used to implement security in cloud storage. Some of the existing encryption Algorithms which were implemented in research work are as follows

A. Data Encryption Standard (DES) Algorithm:

The Data Encryption Standard (DES) is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64- bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds[1]. Each round uses a Different 48-bit round key generated from the cipher key according to a predefined algorithm.

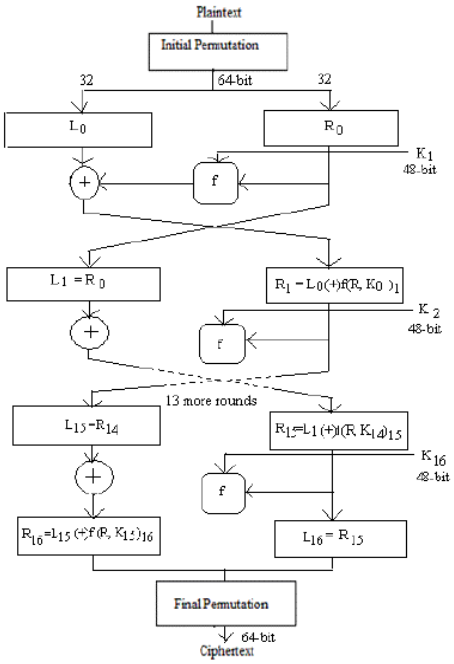


Fig. 2. Encryption with DES

B. RSA Algorithm:

The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is cipher text, then at encryption

C = Memod n

And at decryption side

M = Cd mod n.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-212 PAGE NO: 1321-1328
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Where n is a very large number, created during key generation process.

Key Generation	
Select p, q	p, q both prime, p≠q
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Fig. 3. RSA Algorithm

Hence we propose a system which uses multilevel encryption and decryption to provide more security for Cloud Storage.

A. Proposed System Design:

The proposed system is designed to maintain security of text files only. This proposed system uses DES & RSA algorithm to generate encryption when user uploaded the text files in Cloud Storage and inverse DES & RSA algorithm to generate decryption when user download file from Cloud Storage, for increasing security.

The proposed system is designed to maintain security of text files only. The proposed system design focuses on the following objectives which are helpful in increasing the security of data storage.

B. Proposed Algorithm:

We have proposed a combination of two different security algorithms to eliminate the security challenges of Personal Cloud Storage. We have taken a combination of algorithms like: DES and RSA. DES (Data Encryption Standard) is a symmetric key algorithm, in which a single key is used for both encryption/decryption of data. Whereas RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes.

A user can upload Text file in Personal Cloud Storage. When uploading file DES and RSA Encoding schemes are used to encrypt data. The Block Diagram of proposed work at multilevel encryption

The steps of Multi-level encryption will be as follows;

- Upload the text file.
- Now implementation of DES Algorithm takes place. The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text

The actual key used by DES algorithm for encryption is 56 bits in length. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds.

- DES has 16 rounds, means the main algorithm is repeated 16 times to produce cipher text. As number of rounds increases, the security of system increases exponentially.

Block Diagram of proposed work at multileveldecryption

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-212 PAGE NO: 1321-1328
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

CONCLUSION

Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc.

Cloud Computing can become more secure using cryptographic algorithms. Cryptography is the art or science of keeping messages secure by onverting the data into non readable forms. But the existing cryptographic algorithms are single level encryption algorithms. Cyber criminals can easily cracked single level encryption. Hence we propose a system which uses multilevel encryption and decryption to provide more security for Cloud Storage. As our proposed algorithm is a Multilevel Encryption and Decryption algorithm. Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is expected that using multilevel encryption will provide more security for Cloud Storage than using single level encryption.

VIII. REFERENCES

[1] Sandipan Basu, International Data Encryption Algorithm (IDEA) A Typical Illustration', Journal of Global Research in Computer Science. July (2011) ISSN: 2229-371XVol. 2,

[2] Alexa Huth and James Cebula 'The Basics of Cloud Computing', United States Computer Emergency Readiness Team (2011).

[3]Simar Preet Singh and Gurpinder Singh amra, 'Managing Vulnerabilities' in Cloud Computing', National Conference on Engineering applications' (NCEA-2011), St. Solider Institute of Emerging Technology and Management, alandhar, Punjab. April 9 (2011).

[4] I-Hsun Chuang, Syuan-Hao Li, Kuan-Chieh Huang, Yau-Hwang Kuo," An Effective privacy protection scheme for cloud computing",IEEE 2011.

[5] Jianfeng Yang and Zhibin Chen," Cloud Computing Research and Security Issues", IEEE 2010. Sunita Rani et al, / (IJCSIT) International Journal of Computer Science and Information Technologies,

[6] V. Sandhya, "A Study on Various Security Methods in Cloud Computing", International Journal of Advanced Research in Computer Science, Volume 2, No.6, Nov-Dec 2011.

[7]. Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science and Information Technology, Vol.2(3), 242-249, 2012.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-212 PAGE NO: 1321-1328
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

[8] Birendra Goswani, Dr.S.N.Singh, "Enhancing Security in
Cloud computing using Public Key Cryptography with Matrices", International Journal of Engineering Research and Applications, Vol 2, Issue 4, 339-344, July-Aug 2012.