ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering
SITES
Smart And Innovative Technologies In Engineering And Sciences
Gyan Ganga College of Technology
Vol. 5, Special Issue 3, November 2016

An Efficient Data Security in Cloud Computing Using Encryption Algorithm

Roshni Agarwal

M. Tech (Computer technology and application) Dept of CSE, Gyan Ganga College of Technology, Jabalpur, India

Abstract: Cloud computing is a new era of the modern world. Reasons for development of cloud computing are different people and different purpose depends upon the demand. The improvement of the cloud technology also increases the security issues twice. So we need to solve the security issues in the cloud technology. In this paper, we have discussed about cloud computing security mechanisms and presented the comparative study of several algorithms. In future we are going to propose a new plan to solve security issues for both cloud providers and cloud users.

Keywords: Cloud, Security, Encryption algorithms, Security issues

1. INTRODUCTION

Cloud is a broad solution that delivers IT as a service. Cloud computing is an internet based technology uses the internet & central remote servers to support data and applications. It permits consumers and businesses putting to use without installation and approach their personal files at any computer with internet access. Cloud computing also provided shared resources like electricity distributed on the electrical grid. Before cloud computing, websites and server based applications were executed on a specific system. The cloud computing flexibility is a function of the allocation of resources on authority's request. And the cloud computing provides the act of uniting. The concept of cloud computing is linked closely with those of Information as a service (IaaS), Platform as a service (PaaS), Software as service (SaaS) all of which means a service-oriented architecture. Here comes the first benefit of the cloud computing i.e. it reduces cost of hardware that could have been used at user end. As there is no need to store data at user's end because it is already at some other location.

So instead of buying the whole infrastructure required to run the processes and save bulk of data you are just renting the assets according to your requirement. The similar idea is behind all cloud networks [2]. A cloud is a large pool [1], of easily and accessible virtualized resources, such as hardware, development platforms and/or services.

These resources can be powerfully re-configured to arrange properly to a variable load scale, and also permitting for an optimum resource use. This pool of resources is constituting a type exploited by a pay-per-use model in which guarantees are hold out for acceptance by the infrastructure supply by means of usage Service-Level Agreements(SLA). In the cloud, the end user is just using a very light device which is capable of using a network that connects it to a server at some other location. The users do not need to store the data at its end as all the data is stored on the remote server at some other place. A cloud is a pattern of parallel and distributed system be composed of a collection of interconnected and virtualized computers that are dynamically stipulation and presented as one or more unite computing resources established on service level agreements found amongst negotiation between the service supplier and consumer. It uses remote services through a network using various resources. It is basically meant to give maximum with the minimum resources i.e. the user end is having the minimum hardware requirement but is using the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way.

2. RELATED WORK

In Cloud Storage, any organization's or individual's data can be stored in and accessible from multiple distributed and connected resources or locations that comprises cloud. To provide secured communication over distributed and connected resources, encryption algorithms [6] plays a vital role. It is the basic tool or method for protecting the data.

Encryption algorithm converts the data into scrambled form by using "key" and only authorized user have the key to decrypt the data. In Symmetric key encryption, one key is used to encrypt and decrypt the data. Another technique is known as asymmetric key encryption in which two keys private and public keys are used. Public key is used for encryption and private key is used for decryption [6]. User's data can be made secured in the cloud using encryption. But the question arises that is user's data really encrypted when it is stored in the cloud? If CSP does provide encryption, what encryption algorithm is to be

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering
SITES
Smart And Innovative Technologies In Engineering And Sciences
Gyan Ganga College of Technology
Vol. 5, Special Issue 3, November 2016

used? What is the key's length? Not all encryption algorithms are created equal. Cryptographically, some of the algorithms provide insufficient security; especially non genuine algorithms should not be trusted. Most secure data encryption solutions support all of the major business use cases: full disk encryption [4], database encryption [5], file system encryption [4], distributed storage encryption and even row or column encryption. CSP cannot provide such encryption granularity to each user in each level. In [3], the Advance Encryption Standard is proposed for cloud Security. AES is a block cipher having block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. Generally AES with 128 bit key length is significant. The encryption process contains 10 rounds of processing for 128-bit keys. Except for the last round in each case, all other rounds are identical [1]. 16 byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4-byte words [6]. The 4 x 4 matrix of bytes made from 128-bit input block is referred as the state array. Before any round-based processing for encryption can begin, input state must XORed with the first four words of the schedule.

For encryption, each round consists of the following steps:

- SubBytes – a non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).
- ShiftRows – a transposition step where each row of the state is shifted cyclically a certain number of times
- MixColumns – a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey – each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

In [4], a hybrid approach is used in which two algorithms used one after another to make the encryption complex. It uses advance encryption standard followed by RSA algorithm. An integrated approach is used to secure the data on the cloud using two different techniques. As the double encryption is used by the system, then if the attacker is tries to attack on the data, then it would be difficult for decode the data for the attacker. RSA is used after AES here because there is a big advantage of RSA algorithm. If the attacker may able to decrypts the data of RSA cipher then it will give the results which will be different from the original data. In this hybrid technique the steps that will be performed under the hybrid algorithm are Key Generation, Data Encryption, Private Key Encryption, Private Key Decryption, and Data Decryption. In [3], another hybrid approach is used which is again integration of two algorithm DES (Data encryption standard) and RSA. The proposed system is designed to maintain security of text files or non-text files. This proposed system uses DES & RSA algorithm together to generate encryption when user uploaded the text files in Cloud Storage and inverse the DES & RSA algorithm to generate decryption when user download that file from Cloud Storage, for increasing security[10]. The proposed system is designed to maintain security for text files only. The proposed system design focuses on the following objectives which are helpful in increasing the security of data storage.

1) For Encryption of text files:

- Upload Text file.
- Implementing the DES algorithm of Encryption to generate first level encryption.
- Implementing the RSA algorithm of Encryption to generate second level encryption.
- Store Cipher Text into Database.

2) For Decryption of text files:

- Read Cipher Text from Database.
- Implementing the RSA algorithm of Decryption to generate first level decryption.
- Implementing the DES algorithm of Decryption to generate Plain text.
- Display plain text to user.

3. LITERATURE SURVEY

Table 1: Literature Survey

Title	*Author*	*Conference/Journal*	*Mechanism*	*Limitation*
1] Enhancing Cloud Computing Security using AES Algorithm	AbhaSachdev, MohitBhansali	International Journal of Computer Applications	Uses AES Standards which is block cipher algorithm. Uses 128, 192, or 192 bit key	It requires more computing cost as compared to DES.
2] A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks	Navdeep Singh, Pankaj Deep Kaur	International Journal of Database Theory and Application	It use AES followed by RSA algorithm. AES(128, 192,256 bit key) RSA (1024 bit key).	Most complex system. Need high end processors Need more costly hardware. Time efficiency is less on slow hardware
3] Security in Cloud Computing using Cryptographic Algorithms	Shakeeba S. Khan, Prof.R.R. Tuteja	International Journal of Innovative Research in Computer and Communication Engineering	It uses DES followed by RSA algorithm. DES (64 bit key), RSA (1024 bit key).	DES is weaker than AES. Key size for DES is small, can get access to system under Brute force attack

4. COMPARITIVE DISCUSSIONS

The comparison table considers the important cloud computing security characteristics such as,

- Key used
- Scalability
- Security
- Authentication type

Comparison [7] among the RSA, Homomorphic encryption algorithms and DES, The Homomorphic encryption algorithm and DES are scalable but RSA is not scalable. The security [8], the DES is fully secured for

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

both providers and client side but RSA security applied client side only likewise Homomorphic encryption algorithm security applied cloud itself only. The following table characteristic precedes the insecure issues. So we are using the effective authentication plan to provide stronger security for both cloud providers and consumers.

TABLE
CHARACTERISTICS OF EXISTING ENCRYPTION ALGORITHMS

Character-istics	*DES Algorithm*	*RSA Algorithm*	*Homomorphic Encryption*
Platform	Cloud computing	Cloud computing	Cloud computing
Keys Used	Same key is used for encryption and decryption Purpose.	Different keys are used for encryption and decryption Purpose.	private key is used(without decryption)
Scalability	It is scalable algorithm due to varying the key size and Block size.	Not scalable	scalable decryption
Security applied to	Both providers and client side	Client side only	Cloud providers only
Authentication Type	Message authentication used	Robust authentication implemented	Authentication never used

5. CONCLUSION

This paper is a survey report on various algorithms and combinations for cloud storage security using encryption. It shows the limitations like need of extra processing power or need of high end processors and hardware. It highlights the shortcomings of these some of the algorithms. The future scope of this paper is to overcome these limitations by eliminating the need of high end hardware and securing the cloud data significantly.

REFERENCES

[1] Cloud computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.com.
[2] Cloud computing methodology, systems and applications lizhe wang, rajiv ranjan.http://www.unitiv.com.
[3] AbhaSachdev, MohitBhansali, "Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013.
[4] Navdeep Singh and Pankaj Deep Kaur, "A Hybrid Approach for EncAgudo, Isaac and Nuez, David and Giammatteo, Gabriele and Rizomiliotis, Panagiotis and Lambrinoudakis, Costas. Cryptography Goes to the Cloud. In Lee, Changhoon and Seigneur, Jean-Marc and Park, James J. and Wagner, Roland R., editors, Secure and Trust Computing,
[5] Heidelberg, 2011.rypting Data on Cloud to prevent DoS Attacks", International Journal of Database Theory and Application Vol.8, No.3 (2015), pp.145-154.
[6] Shakeeba S. Khan, Prof.R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization)
[7] Vamsee Krishna Yarlagadda and Sriram Ramanajum, "Data Security in Cloud Computing", Vol.2 (1), p.p (15-23) (2011).
[8] Veerraju Gampala, Srilakshmi Inuganti and Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.