A Survey on Data Security in Cloud Computing

Parekh Devangi Sunilkumar
Department of Computer Engineering
GEC, Gandhinagar, India

Abstract— Cloud computing is an information technology paradigm that enables ubiquitous access to shared resources and higher-level services that can be easily provide by minimum management effort, often over the Internet. The cloud aims to low costs, and helps the users focus on their core business instead of being impeded by IT obstacles. The main technology for cloud computing is virtualization. Virtualization software separates a physical computing device into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. It provides lots of benefits such as simplicity and lower costs, almost unlimited storage, least maintenance, easy utilization, backup and recovery, continuous availability, quality of service, scalability, flexibility and reliability, easy access to information. While there is increasing use of cloud computing service in this new era, the security issues of the cloud computing become a challenges. Security is one of the most critical aspect in cloud computing due to the sensitivity of user's data. Cloud computing must be safe and secure enough to ensure the privacy of the users. This paper firstly lists out parameter that affecting to cloud computing, then discuss the most common used security algorithm to secure the data of cloud computing.

Key words: Cloud Computing, Security Algothims, AES

I. INTRODUCTION

Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Main goal of the cloud computing is to provide scalable and on-demand computing infrastructures, good quality of service levels. Security, reliability, cost, virtualization, need, on demand service, maintenance, integration are main part of security of cloud computing. cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is latest development that provides easy access to high performance computing resources and storage infrastructure through web services. Cloud computing delivers the potential for efficiency, cost savings and improved performance to governments, organizations, private and individual users. It also offers a unique opportunity to developing countries to get closer to developed countries. The paper addresses the parameter affected to cloud computing[3]. After identify these, some comparison between security algorithms and finally discussed the AES algorithm[2].

II. LITERATURE REVIEW

A. *Parameter Affecting to Cloud Computing*

Cloud computing has various characteristics. Users' need can change dynamically and cloud computing enables users to consume computing resources such as software and storage when they are required and users only buy according to their needs and they are charged by the amount that they used and this is on demand service characteristics of cloud computing

This characteristic of cloud computing relies on virtualization. Cloud computing also enables organizations to store their servers, other hardware and equipments virtually instead of physically[3].

Cost is also one of the most important characteristics of cloud computing. Cost consists of purchasing cost and long term usage costs. Purchasing cost of cloud computing is very inexpensive compared to traditional computer technologies. Consumers have benefit of low cost advantage of cloud computing because buying services over cloud computing is particularly inexpensive.

In addition, companies can save in energy, space and staff by preferring cloud computing technologies. In other words, in the long run organizations save in costs. The responsibility to update applications and software belongs to cloud service provider and it decreases software upgrade costs of an organization. Moreover, they save in maintenance costs by reducing the number of both actual hardware and maintenance staff. In this manner, maintenance is very easier because in an organization, because updates and other maintenance processes are held in the cloud rather than on each user's computers[3].

Security is another issue related to cloud computing. Security is evaluated a cloud computing risk by organizations. Customers or cloud users must be sure that their organizational data is more secure in a cloud.

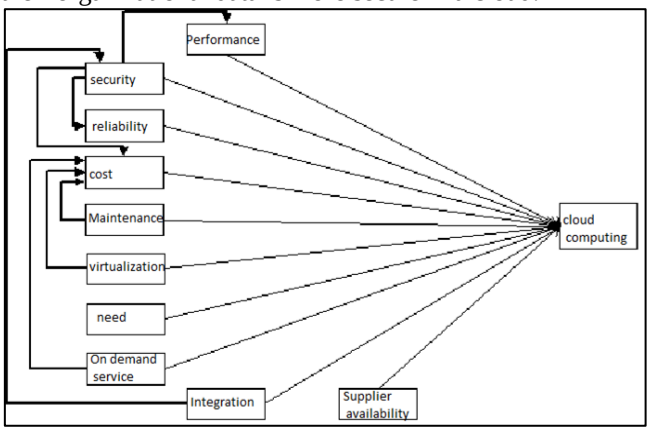

Fig. 1: Theoretical Framework of Study

B. *Security Algorithm*

As the central data storage is the key facility of the cloud computing it is of prominent importance to provide the security. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography[2].

Security goals of data cover three points namely: Availability, Confidentiality, and Integrity. Cryptography, in modern days is considered grouping of three types of algorithms[5]. They are

1) Symmetric-key algorithms
2) Asymmetric-key algorithms
3) Hash functions

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys [citation needed]. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. Examples of popular symmetric-key algorithms include Twofish, AES, Blowfish, CAST5, Kuznyechik, RC4, DES, and Skipjack.

Asymmetrical cryptography is any cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. This accomplishes two functions: authentication, which is when the public key is used to verify that a holder of the paired private key sent the message, and encryption, whereby only the holder of the paired private key can decrypt the message encrypted with the public key. It comprises various algorithms like Rivest, Shamir, & Adleman (RSA), Digital Signature Algorithm (DSA), Elliptic Curve (EC), Diffi-Hillman (DH), El Gamal etc.

The Hash functions use a mathematical transformation to irreversibly "encrypt" information. It contains algorithms like Message Digest, Secure Hash Algorithm.

We choose symmetric cryptosystem as solution as it has the speed and computational efficiency to handle encryption of large volumes of data. In symmetric cryptosystems, the longer the key length, the stronger the encryption.

AES is most frequently used encryption algorithm today this algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte. As of today, no practicable attack against AES exists. Therefore, AES remains the preferred encryption standard for governments, banks and high security systems around the world[1].

A privacy-preserving public auditing system for data storage security in cloud computing is intended, although the computational time is increased but the privacy is preserved where data is stored in the cloud by using the most prominent algorithm AES.

In AES data encryption is more scientifically capable and graceful cryptographic algorithm, but its main force rests in the key length. The time necessary to break an encryption algorithm is straight related to the length of the key used to secure the communication. AES allows choosing a various type of bits like 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES. It is described a new architecture for security of data storage in multicloud. Two mechanisms-data encryption and file splitting are used. When user uploads a file, it is encrypted using AES encryption algorithm. Then that encrypted file is divided into equal parts according to the number of clouds and stored into multicloud. This proposed system enhances the data security in multicloud.

Based on the text files used and the experimental result it was concluded that AES Algorithm consumes least encryption and RSA consume longest encryption time. They also observed that Decryption of AES algorithm is better than other algorithms. From the simulation result, they evaluated that AES algorithm is much better than DES and RSA algorithm.

C. AES Algorithm

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES[1].

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

1) Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations) [1].

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration

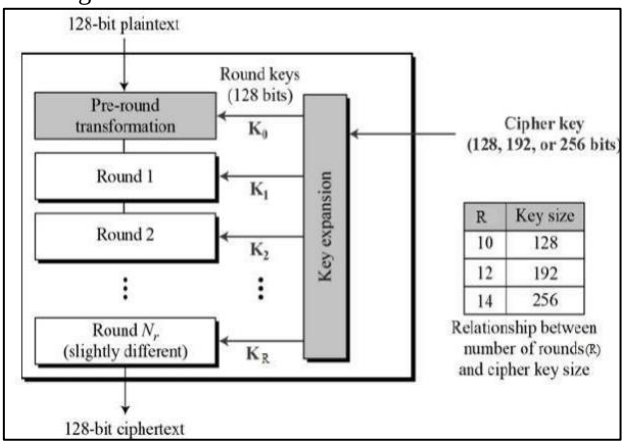

Fig. 2: AES Structure

2) Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below

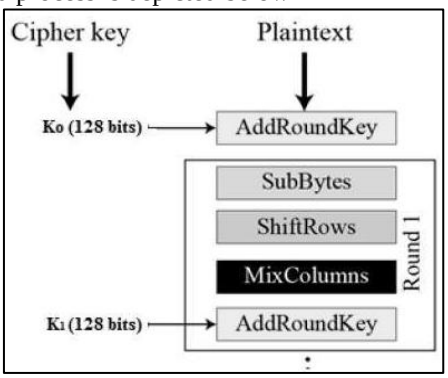

Fig. 3: Encryption Process

3) Byte Substitution (Sub Bytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

4) Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

5) Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

6) Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

7) Decryption Process

The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order

- Add round key
- Mix columns
- Shift rows
- Byte substitution

8) AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches[1].

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

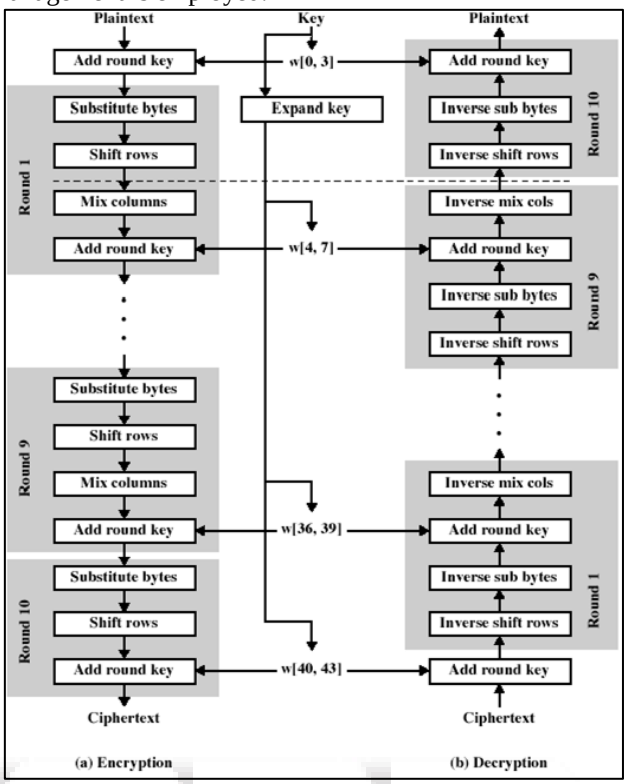

Fig. 4: Process of AES Algorithm

III. CONCLUSION

Cloud computing is latest technology that is being widely used all over the world. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography. This paper surveyed different techniques about data security and privacy, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments to build trust between cloud service providers and consumers.

REFERENCES

[1] Enhancement of Cloud Computing Security with Secure Data Storage using AES IJIRST –International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 09 | February 2016.

[2] Data Security in Cloud Computing International Journal of Current Trends in Engineering & Research (IJCTER) e-ISSN 2455–1392 Volume 2 Issue 4, April 2016.

[3] Factors Affecting the Adoption of Cloud Computing, researchgate conference paper,2012

[4] Cryptographic Protocols for Secure Cloud Computing International Journal of Security and Its Applications Vol. 10, No. 2 (2016).

[5] Security Techniques for Data Protection in Cloud Computing International Journal of Grid and Distributed Computing Vol. 9, No. 1 (2016).

[6] Harjit Singh Lamba and Gurdev Singh, ―Cloud Computing-Future Framework for emanagement of

NGO's‖, IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[7] Dr. Gurdev Singh, Shanu Sood, Amit Sharma, ―CM-Measurement Facets for Cloud Performance‖, IJCA, Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[8] Rabi Prasad Padhy, Manas Ranjan Patra , Suresh Chandra Satapathy, ―Cloud Computing: Security Issues and Research Challenges‖, International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[9] Prince Jain, ―Security Issues and their Solution in Cloud Computing‖, International Journal of Computing & Business Research, Proceedings of ‗I-Society 2012‘at GKU.

[10] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, DR. Atanu Rakshit, ―Cloud Security Issues‖, 2009 IEEE International Conference on Services Computing.

