IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. V (Mar – Apr. 2015), PP 110-114
www.iosrjournals.org

Enhancing Cloud Computing Security for Data Sharing Within Group Members

P.Krithika[1], G.Linga Dilipan[2] , M.Shobana[3]
[1](*Department Of Computer Science And Engineering,SNS College Of Technology,Anna University,India)*
2*(Department Of Computer Science And Engineering,SNSCollege Of Technology,AnnaUniversity,India)*
3*(Department Of Computer Science And Engineering,SNSCollege Of Technology,AnnaUniversity,India)*

Abstract: *In cloud computing , the following security functions are commonly considered are as follows, Cloud Data confidentiality ensures the owner that the stored data can be accessed only by an intended user and Cloud Data authentication ensures the group member that the data was accessed by a specified owner and the data was not altered en route. To provide these two functions,the Dynamic Group key protocol relies on one trusted entity, KGC (Key Generation Center), to choose the key, which is then transported to involved members. System uses interval based Interval Based algorithm for re-keying which not only reduce the key generation and sharing complexity, but also improves the owner data sharing efficiency and security.The main security goals for dynamic group key based data sharing in cloud to encrypt the data before sharing. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.The goal is to secure the data sharing within group members,comparing AES algorithm with other encrypted algorithm and to analysis which algorithm suits for encrypting the data.*

Keywords: *Bit Mangling , Cipher, Cryptanalysis.*

I. Introduction

Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications.In cloud computing,[1] the word cloud is used to denote the metaphor "The Internet" so the wordcloud computing means "Cloud computing is a large pool of systems where it is connected in private or public networksinorder to provide dynamically scalable infrastructure for application, data and file storage - are delivered to an organization's computers and devices through the InternetSecurity issues in cloud computing has played a major role in slowing down its acceptance, in fact security is a main issue in cloud computing.

II. Issues

Some of the issues appear in the cloud computing are:

- **Identity privacy:**

The problem in adopting cloud computing is identity privacy.In cloud computing [2] without assurance of identity privacy,there is little doubt to join in this,because the privacy are not maintained properly ,the identities of the user can be disclosed to various kinds of intruders and cloud service providers(CSP).

- **No Multiple-owner manner:**

The single owner can be able to store and modify the data file because it is less flexible than multiple-owner.In amultiple-owner manner the member can able to read the data and alter their data files but the group manager can store and modify data in the cloud.

- **Effect of Dynamic Groups:**

Primarily, new granted users are not allowed to read the content of data files stored before their participation by the anonymous system, because itimpossible management it is desirable to obtain an efficient membership.

Here is the graphical representation of survey ranking security challenges:

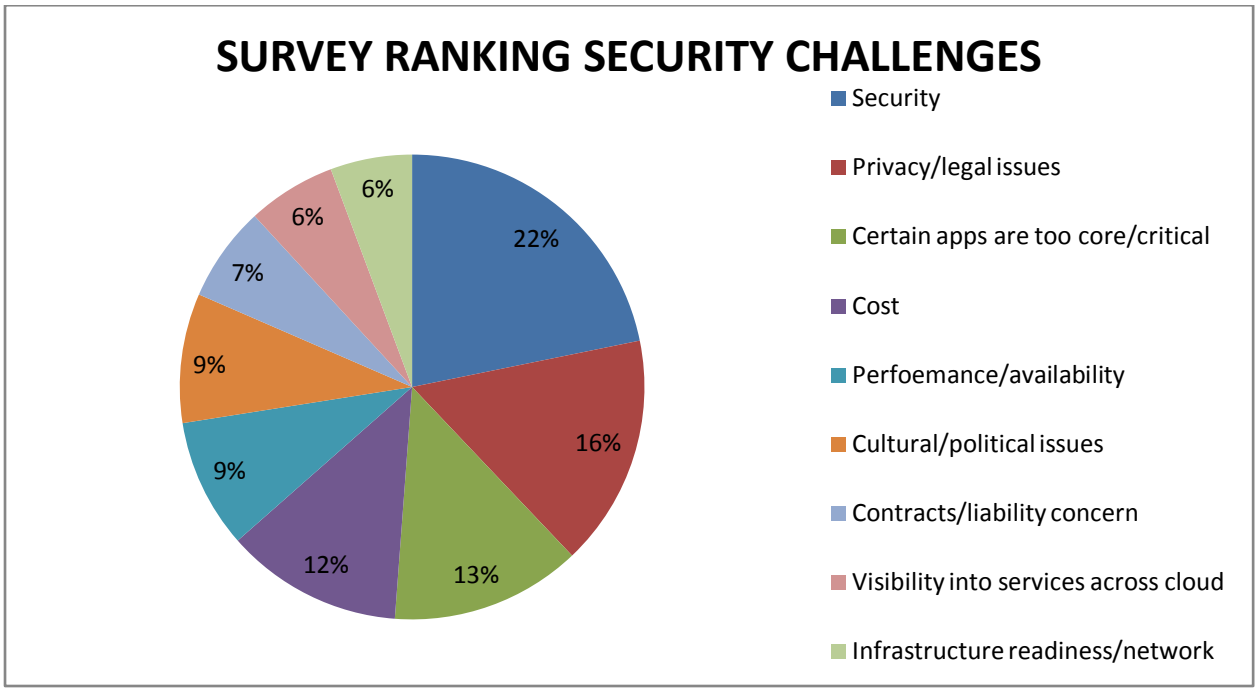

Figure 1: Results of survey ranking security challenges

From above figure,[3] security could improve due to centralization of data and increased security-focused resources. On the other hand, there is a loss of control over certain data, and the lack of security for storing kernels entrusted to cloud providers. If cloud providers have not done good jobs in securing their own environments, the consumers may be at risk. Measuring the quality of cloud providers the security is more difficult because many cloud providers will not expose their infrastructure to customers. This is a survey were more specific to the different security issues and the associated challenges that has been in the cloud computing system.

III. Types of Clouds

There are various types of cloud they are:

1.Public cloud: It is the one of the cloud inwhere the cloud services are being available tousers via a service provider over the Internet.It provides a control mechanism to the users.

2.Private Cloud: It provides many advantages over public cloud , but the main difference between public and private cloud is that the data is managed properly within the organization only, without the limits of network bandwidth.

3.Community Cloud: It is basically managed by a group of originations that have a common objective to achieve. The members can share and access the data in the cloud.

4.Hybrid Cloud: This is the combination of both public and private cloud. It is defined as multiple cloud systems,where they are connected in a way that allows programs and data to be moved easily from one system to another.

IV. Comparison

In cloud computing,for securing the data sharing within agroup members, we can encrypt the data using various encryption algorithm such as AES,DES,RSA,Blowfish and Broadcast algorithm.By considering any two algorithms we can justify which algorithm is suitable for data sharing within a group members.Here we are going to consider about AES and other encrypted algorithms.

V. AES Algorithm

AES is a block cipher with a block length of about 128 bits. It allows three various key lengths they are128 ,192 and 256 bits.

We used [5] AES with 128 bit key length. The encryption process for128-bit keys consists of 10 rounds.

16 byte encryption key, in the form of 4-byte words are expanded into a key schedule consisting of 44 4-byte words. The 4 x 4 matrix of bytes made from 128-bit input block is referred to as the state array.Encryption can begin for any round-based processing , the first four words of the schedule is XORed for input state.

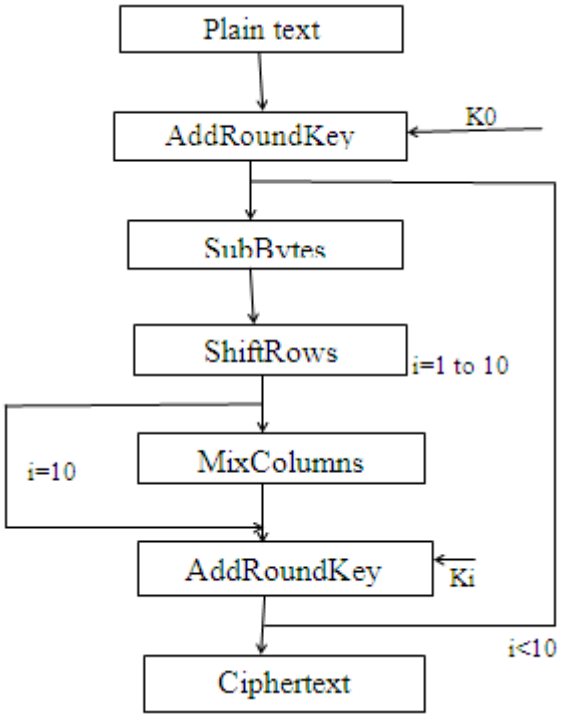

Figure 2: The flowchart of AES Encryption algorithm

For encrypting , each round consist of the following four steps:

1.Sub Bytes

This step involves sample resistance from differential and linear cryptanalysis attacks. SubByte is byte-by-byte substitution where each byte is substituted independently using Substitution table (S-box). In SubBytes each input byte is partitioned into 24-bit patterns, each representing an integer value between 0 and 15 which can be then interpreted as hexadecimal values. Left digit contains the row index and the right digit contains the column index of S-box. At the intersection of row and column,the value given is substituted. There can be possible of sixteen distinct byte-by-byte substitutions. It is constructed by a combining of GF (28) arithmetic and bit mangling.

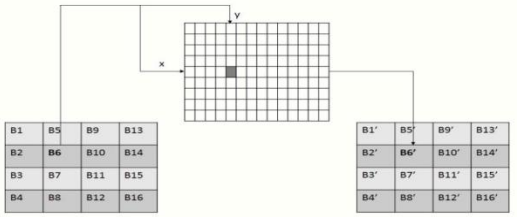

Figure 3: Sub Bytes Transformation Step

2.Shift Rows

The purpose of this step is to provide diffusion of the bits over multiple rounds. First,the row 0 in the matrix is not shifted, row 1 is circular left shifted by one byte, next row 2 is circular left shifted by two bytes, and then row 3 is circular left shifted by three bytes.

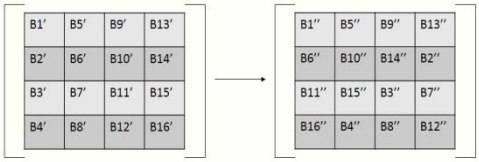

Figure 4: ShiftRows Transformation Step

3.Mix Columns

Like previous step, the purpose of this step is to provide diffusion of the bits over multiple rounds. This is achieved by performing multiplication one column at a time. Each value in the column is multiplied with every row value of a standard matrix. Then,the results of these multiplications are XORed together. For e.g. value of first byte B1'' is multiplied by 02, 03, 01 and 01 and XORed to produce new' B1' of resulting matrix. The multiplication continues again one matrix row at a time against each value of a state column.

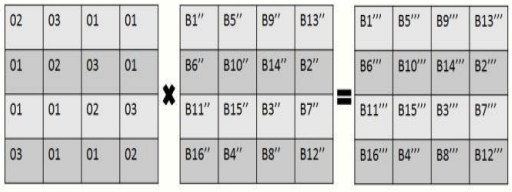

Figure 5: MixColumns Transformation Step

4.Add RoundKey

In this step, the matrix is XORed with the round key. The original key contains 128 bits/16 bytes which are represented in the form of 4x4 matrix. This 4 words key where each word will have 4 bytes,then it converts to a 43 words key.

VI. Comparing Aes With Other Algorithms

The fact that the cipher and its inverse use different components practically eliminates the possibility for weak and semi-weak keys in AES, which is an existing drawback of DES. Also, the nonlinearity of the key expansion practically eliminates the possibility of equivalent keys inthe AES. A performance comparison the encrypted algorithm such as AES, DES[6] and Triple DES for different microcontrollers shows that AES has a computational cost of the same order as required for Triple DES . Another performance evaluation reveals that AES has an advantage over algorithms-3DES, DES and RC2 in terms of execution time (in milliseconds) with different packet size and throughput (Megabyte/Sec) of encryption as well as decryption. Also in the case of changing data type such as image instead of text, it has been found that AES has an advantage over RC2, RC6 and Blowfish in terms of consuming time[7].

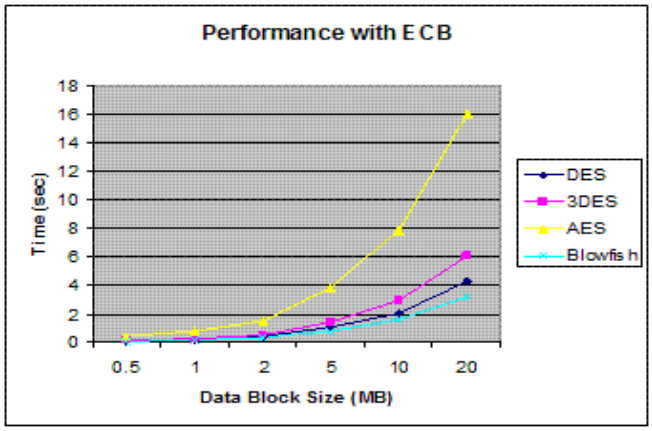

Figure 6:Comparison of Time and Block Size.

The key-size of the algorithms may vary. Like-Key size of Blowfish algorithm contains128 to 448 bits and AES algorithm contains 128,192,256 bits. The key length of AES is less than Blowfish. 2048 bits of asymmetric key are equivalent to 112 bits of symmetric key.

VII. Conclusion

According to report,security plays a major role in data sharing[8] within a group members.The user can avail cloud services[9] and cloud providers have a justify security issue.

AES algorithm is used to encrypt the data before sharing the data within a group members.AES algorithm performs well in both hardware and software when comparing to other encrypted algorithms.It requires only less memory consumption and there is no serious weak keys in the AES.It supports any block size and key sizes.

According to AES algorithm is better than other algorithms. Though each cloud infrastructure has its own security strengths; the user can choose infrastructure according to his security requirements.[10] AES provides security to cloud users as encrypted data in the cloud is safe from many attacks.

References

[1]. Armbrust. M, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[2]. Xuefeng Liu, Yuqing Zhang, Boyang Wang, and JingboYan,"Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL.24, NO. 6, JUNE 2013

[3]. F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges",IDCeXchange, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].

[4]. MohitBhansali and AbhaSachde"Enhancing Cloud Computing Security using AES Algorithm"International Journal of computer apllications(0975 – 8887) Volume 67- No.9, April 2013.

[5]. NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001 [Online]. Available:http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[6]. Sanchez-Avila, C., and R. Sanchez-Reillol. "The Rijndael block cipher (AES proposal): a comparison with DES." Security Technology, 2001 IEEE 35th International Carnahan Conference on. IEEE, 2001

[7]. Elminaam, DiaaSalama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud."Performance Evaluation of Symmetric Encryption Algorithms." IJCSNS International Journal of Computer Science and Network Security 8.12 (2008): 280-286.

[8]. Enterprise and Individual Users to fuel Growth in Cloud Computing [Online]. Available:http://www.redorbit.com/news/technology/1112692915/cloud-computing-growth-paas-saas-091212/

[9]. Worldwide and Regional Public IT Cloud Services 2012-2016 Forecast [Online]. Available:http://www.idc.com/getdoc.jsp?containerId=236552.

[10]. John Harauz, Lori M. Kaufman and Bruce Potter, ―Data security in the world of cloud computing ―, 2009 IEEE CO Published by the IEEE Computer and Reliability.