AN IMPROVISED SECURITY FOR CLOUD COMPUTING

[1]*K.VENKATA NARASA RAJU* [2]*Dr.D.MALATHI*
[1]M.Tech Student, Department of Computer Science and Engineering,
SRM University Kattankulathur, Chennai.
[2]Professor, Department of Computer science and Engineering,
SRM University,Kattankulathur, Chennai.

ABSTRACT-

In past three decades, the world of computation has changed from centralized (client-server not web-based) to distributed systems and now we are getting back to the virtual centralization (Cloud Computing). Location of data and processes makes the difference in the realm of computation. On one hand, an individual has full control on data and processes in his/her computer. On the other hand, we have the cloud computing wherein, the service and data maintenance is provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. So, logically speaking, the client has no control over it. The cloud computing uses the internet as the communication media. When we look at the security of data in the cloud computing, the vendor has to provide some assurance in service level agreements (SLA) to convince the customer on security issues. In cloud computing, data will be stored in the storage provided by the service providers. Service providers must have a practical way to protect their customers' data, in particular to prevent data disclosure by unauthorized insiders. Store data in encrypted form is a common method of protecting information privacy. If a cloud system is responsible for tasks on the storage and encryption / decryption of data, system administrators can concurrently get the encrypted data and decryption keys. This allows them to access information without authorization and therefore poses a risk to the privacy of information. Therefore, this paper aims to enable the user to make his own encryption / decryption for achieving improvised security.

1. INTRODUCTION

Weiss noted that cloud computing services include several existing computing technologies, such as service-oriented utility computing, grid computing with large amount of computing resources, and that using data centres for data storage services.

Critical industrial data was stored internally on storage media, protected by security measures including firewalls to prevent external access to the data and including organizational regulations to prohibit unauthorized internal access. In the cloud computing environment, storage service providers must have in place data security practices to ensure that their clients' data is safe from unauthorized access and disclosure. More importantly, the regulations and measures for preventing privileged users such as system administrators from unauthorized access must be rigorously established and implemented.

Service providers follow specific policies and practices to protect their users' data, and these policies are usually stated in the service contract. In a cloud computing environment, the service content offered by service providers can be adjusted according to the needs of the user. Generally, these service agreements are referred to as Service Level Agreements (SLA). By signing an SLA, the user shows that he has understood and agreed to the contents of the application service, and agrees with the provider's data privacy and protection policies.

A common approach to protect user data is that user data is encrypted before it is stored. In a cloud computing environment, a user's data can also be stored following additional encryption, but if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption keys and internal access privileges to access user data. From the user's perspective, this could put his stored data at risk of unauthorized disclosure.

Creating user trust through the protection of user's data content is the key to the widespread acceptance of the cloud computing. This study proposes a business model for cloud computing based on the concept of using a separate encryption and decryption service. In the model, data storage and decryption of user data are provided separately by two distinct providers. In addition, those working with the data storage system will have no access to decrypted user data, and those working with user data encryption and decryption will delete all encrypted and decrypted user data after transferring the encrypted data to the system of the data storage service provider.

The data storage cloud system provider is authorized to store the user's encrypted data, but does not have access to the Decryption Key. Thus, the storage system can only retrieve encrypted user data, but is unable to decrypt it. The cloud computing system responsible for encrypting user data has authority over all encryption keys required for data encryption but, given that the encryption provider does not store the user's data, internal mismanagement of the decryption keys still poses no risk of unauthorized disclosure of the user's data.

Given that encryption is an independent cloud computing service, a unique feature of the business model is that different services are provided by multiple operators. For example, the Encryption as a Service provider and the "Storage as a Service" provider cooperate to provide a Cloud Storage System with effective data protection. This study provides a draft SLA for this type of business model of combining multiple providers in a single service, which can establish the cooperation model between operators and the division of responsibility for the services they jointly provide to the user.

2. PROPOSED SYSTEM

In proposed method, the user will be doing his/her own Encryption/Decryption. After the completion of Encryption service it will be forwarded to storage service provider. Then, finally it is forwarded to corresponding storage of service provider. Fig.1. shows this process.

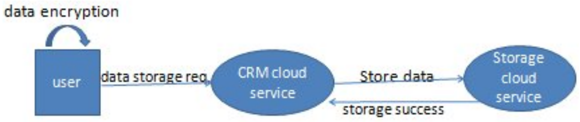

Fig.1: Storing of data in cloud

Similarly, for retrieving the data from cloud storage as shown in fig.2, the user first login to the cloud service provider and then send request to cloud storage service. Now the cloud storage provider sends encrypted file to cloud service provider and the provider forwards the file to user. Now the user does decryption and reads the file.

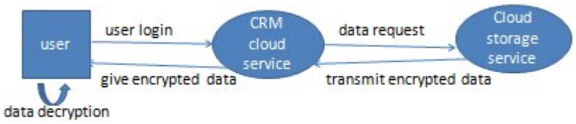

Fig.2: Retrieving data from cloud

Multiphase Encryption:

Diffie and Hellman have argued that the 56-bit key used in the Federal Data Encryption Standard (DES) is too small and that current technology allows an exhaustive search of the 256 keys. Although there is controversy surrounding this issue, there is almost universal agreement that multiple encryption using independent keys can increase the strength of DES [5].

Multiple encryption as found in 3DES and AES provides cryptographic assurance of a message's integrity. The simplest approach to increasing the key size is to encrypt twice, with two independent keys $K1$ and $K2$. Letting P be a 64-bit plaintext, C a 64-bit ciphertext, and K a 56-bit key, the basic DES encryption operation can be represented as

C= S_k (P), and simple double encryption is obtained as C=S_{k2} [S_{k1} (P)].

While exhaustive search over all mentioned keys (K1-K2 pairs) requires more operations and is clearly infeasible, this cipher can be broken under a known plaintext attack (where corresponding plaintext and cipher text are both known) with 2^{56} operations [6]. The time required is therefore no greater than is needed to cryptanalyze a single 56-bit key exhaustively (although there is very significant additional cost for memory). If *P* and *C* represent a known plaintext--ciphertext pair, then the algorithm for accomplishing this double encryption encrypts *P* under all 2^{56} possible values of *K*1, decrypts *C* under all 2^{56} values of *K*2, and looks for a match. For obvious reasons, this is called a "meet in the middle" attack [7].

Triple DES uses a "key bundle" which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits.

The encryption algorithm is:

ciphertext = E_{K3}(D_{K2}(E_{K1}(plaintext)))
I.e., DES encrypts with K_1, DES decrypt with K_2, then DES encrypt with K_3.

Decryption is the reverse:
plaintext = D_{K1}(E_{K2}(D_{K3}(ciphertext)))
I.e., decrypt with K_3, *encrypt* with K_2, then decrypt with K_1.

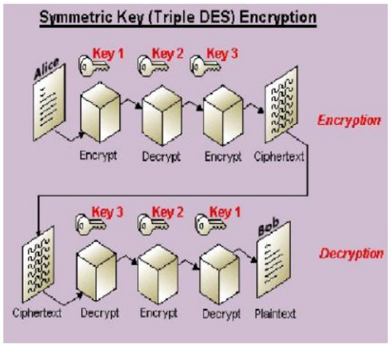

Fig. 3. Description of multiple encryption (triple DES)

In Fig. 3, the whole process of Triple DES is described. Each triple encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using a set of different keys instead of symmetric keys [8].

3. OVERVIEW OF THE PROPOSED ENCRYPTION TECHNIQUE

This idea differs with existing data encryption techniques to provide network and information security over the wireless network. It may create complexity of data encryption number of times due to performing the same operation multiple times with different encryption key in existing way. As per cryptographic protocol, more and more complexity in data encryption technique enhances the security of data transmission over the wireless channel. Large number of encryption of encrypted data will increase the complexity of data encryption enormously, which will be very complicated to decrypt it.

A. Example

Complexity of Existing Encryption Technique / method
(Multiple Encryption) = *O* (*N***N**…………**N*)
Complexity of New (As per proposed idea) Encryption
Technique = *O* (*N***N**………**N*) * *O* (*N***N**…..**N*) *……………………………* *O* (*N***N**…..**N*).
(Depending upon the multiplicity of the Encryption Technique involved.)

B. Conventional Encryption Technique (Using Ceaser Cipher Encryption Technique)

Original Data/ Plain Text – GURUKULA
Algorithm – *C* = *P* + 3 (Key as Second successor of
plaintext)
Cipher Text – JXUXNXOD

C. Multiple and Multiphase Encryption Technique

In cryptography, by encrypting a message twice with some block cipher, either with the same key or by using two different keys, then we would expect the resultant encryption to be stronger in all but some exceptional circumstances. And by using three encryptions, we would expect to achieve a yet greater level of security.

For instance, the use of double encryption does not provide the expected increase in security when compared with the increased implementation requirements, and it cannot be recommended as a good alternative. Instead, triple-encryption is the point at which multiple encryptions give substantial improvements in security.

Example:
Original Data/ Plain Text – GURUKULA
Algorithm – $C = ((P + 3) + 3) + 3$ ………… + 3) (N Times)
Cipher Text –
JKOCPUJW (After First Cycle)
MNRFSXMZ (After Second Cycle)
PQUIVAPC (After Third Cycle)
…………………………………….
……………………………………..
Encrypted N Times

In such a way, multiple encryptions will occur in each phase and this process will be repeated number of times up to desired extent. So, multi-phase encryption comprises number of such phases which are strongly protected due to multiple encryption in each phase.

Multi-phase Data Encryption describes the enhanced complexity of data encryption due to performing the same operation multiple times in existing way (single phase encryption techniques).

Example:
Original Data/ Plain Text – GURUKULA
Algorithm – $C = ((P + 1) + 3) + 5$ ………….. (N Times)
Cipher Text –
HVSVLVMB (After First Cycle)
KYVYOYPE (After Second Cycle)
PDADTDUJ (After Third Cycle)
…………………………………….
……………………………………..
Encrypted N Times

In such a way, multiple encryption occurs with different encryption keys (encryption algorithms) in each phase of multiphase encryption.

In the single phase of multiphase encryption is described as multiple encryption where at each cycle different encryption key is used. In this encryption technique, decryption will be performed in reverse order. In multiphase encryption, such processes will be repeated number of times to enhance the complexity in encryption/decryption as well as security of data.

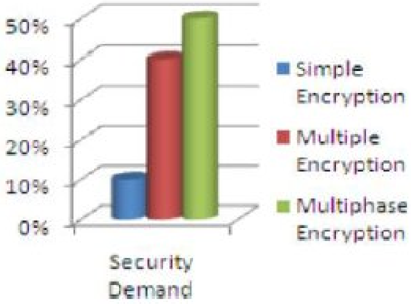

Fig. 4. Security demand of various encryptions

In this figure, as per general survey we can see that the demand of multiphase encryption is increasing day by day in comparison of other simple & multiple encryption techniques to enhance the security in data communication over wireless network.

Applied Cryptography includes the source code for DES, IDEA, BLOWFISH, RC5 and other algorithms [9]. In current scenario, the source code for multiphase encryption will increase the popularity of Applied Cryptography for the enhancement of data security. At the initial stage, the implementation of multiphase encryption may be complex but it will enhance the security of data communication enormously.

Cryptographic algorithms and key sizes have been selected for consistency and to ensure adequate cryptographic strength for Personal Identity Verification (PIV) applications [11]. Multiphase encryption may reduce the problem of key management in the existing technology of Personal Identity Verification (PIV) due to use of different encryption algorithms with fixed size keys instead of large number of variable length keys.

4. CONCLUSION

In traditional method there will be third party who will be handling encryption or decryption using some encryption/decryption techniques may capable of retrieving data. So, we proposed a method in which the user can do his/ her own encryption or decryption by using multiphase encryption which provides high security compared to others.

5. REFERENCES

[1] Jing-Jang Hwang and Hung-Kai Chuang and Yi-Chang Hsu and Chien-Hsing Wu "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service"

[2] A. Weiss, "Computing in the clouds", netWorker, vol. 11, no. 4, pp. 16- 25, December 2007.

[3] C. S. Yeo, S. Venugopal, X. Chu, and R. Buyya, "Autonomic metered pricing for a utility computing service", Future Generation Computer Systems, vol. 26, issue 8, pp. 1368-1380, October 2010.

[4] M. Baker, R. Buyya, and D. Laforenza, "Grids and grid technologies for wide-area distributed computing," International Journal of Software: Practice and Experience, vol.32, pp. 1437-1466, 2002.

[5] R. C. Merkle and M. E. Hellman, ―On the security of multiple encryption, *Department of Electrical Engineering, Stanford*, CA published in ACM, A technical note on Programming Technique & Data Structure in Stanford University, vol. 24, no. 7, 1981.

[6] W. Diffie and M. Hellman, ―New directions in cryptography, *IEEE Trans. Info*., vol. 22, no. 6, pp. 644-654, Nov. 1976.

[7] P. V. Oorschot and M. J. Wiener, *A Known-Plaintext Attack onTwo-Key Triple Encryption*, EUROCRYPT'90, LNCS 473, 1990, pp. 318-325.

[8] L. M. Vaquero,L. Rodero-Merino,J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.

[9] B. Schneier, ―Applied cryptography second edition: protocols, algorithms, and source code in C, *John Wiley and Sons*, 1996, pp. 758..

[10] Himanshu Gupta and Vinod Kumar Sharma "Multiphase Encryption: A New Concept in Modern Cryptography", Vol. 5, No. 4, August 2013

[11] NIST Special Publication 800-78-2, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, February 2010