SECURED DATA OVER CLOUD WITH CRYPTOGRAPHY

K.Monica[1], T.Ramarao[2], Ch. Ashok [3]

Assistant Professor[1], Assistant Professor[2], Assistant Professor [3]

Department of Computer Science & Engineering,

Godavari Institute of Engineering & Technology, Rajahmundry

ABSTRACT:

It is known that cloud is the emerging technology for providing data access in a dispute free manner. Though there are lot many advantages in using cloud for service enterprise, it is equally essential to protect data from being running into the hands of intruders. In order to protect data from intruders and to promote safe transmission of data, security is needed and also the vendor of the cloud is responsible for providing accountability to the user such as on which machine the data is transmitted and so on.This accountability led to the introduction of log mechanism that keeps track of the data being used. Thus reducing the fear of secured data being going into wrong transactions. This is done with the introduction of object centralized approach that includes the enclosing of users data with policies. We use JAR programs to achieve this by triggering an authentication page for every access of information in the cloud. Thus making the cloud transparent to the users. Security is being provided by using both cryptography and steganography together. Where Cryptography is used for safe transmissions which includes usage of different keys for both encryption and decryption in other hand. Therefore using this technologies together results in the double security to the data being transmitted.

Keywords: Cryptography, 3DES, CIA, etc.,

1. INTRODUCTION

Cloud computing presents the new way of supplementing the current usage and delivery of the software (IT) over the Internet. It is done by dynamically providing scalable and virtualized resources as a service to the customers. Up to now there are number of commercial cloud computing services like Amazon, Yahoo, and Microsoft and so on. Though its making the transactions easier it lacks behind to satisfy the user criteria of providing details regarding the machine on which the data is being processed. This lack of information regarding what purpose the data has been used and on what machine it’s been processed, the user feels a fear of losing control over his own personal data or financial data. This becomes an obstacle for better utilization of cloud by many customers. This can be avoided by using CIA frame work which is based on the concept of information accountability [2].This provides an end-end accountability in the cloud. By the means of CIA [3] the owners can track whether their agreement which is made at the very initial step of service is being honored or not. The Cloud Information Accountability frame work came out with a novel approach where the user can track the usage of his data at his desired step of the process. Thus making the approach transparent to the user. In associated with the accountability feature we can use adopt two distinct modes like push mode and pull mode. These two modes play a vital role in auditing. This entire thing is carried out with the use of JAR programming capabilities.

The security is provided by using cryptography which includes both usage of two different keys namely:

- Asymmetric Key Cryptography
- Symmetric Key Cryptography.

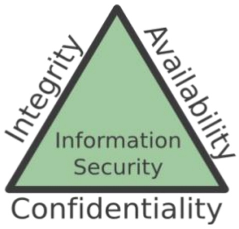
- **Asymmetric Key Cryptography:** The technique where different keys are used for both encrypting and decrypting the information is known as Asymmetric Key Cryptography
- **Symmetric Key Cryptography:** The technique where same key is used for both encrypting and decrypting the information is known as Symmetric Key Cryptography.

The main aspects cryptography deal is to satisfy its goals in terms of data namely:

- Confidentiality
- Integrity
- Authentication.

- **Confidentiality:** The principle confidentiality is that only sender and the intended recipient should be able to access the contents of the message.
- **Integrity:** The contents of the message should not be changed in the middle of the transmission. The sender sends the message and the contents of the message is changed before it reaches the intended recipient then we can say that integrity is lost in this case.
- **Availability**: The principle availability is that resources should be available to authorized parties at all times.

CIA Architecture:



Cryptography includes the following components:

- **Plain text:** Original message that is fed into algorithm.
- **Encryption algorithm:** It performs various substitution and transformation.
- **Secret Key:** This is the input to the algorithm and key is a value independent of plain text.
- **Cipher text:** The transformed text is called Cipher text
- **Decryption algorithm:** The reverse of encryption algorithm

2. LITERATURE SURVEY

In this section we will have a clear glance over the security addressing related works in the cloud. We have got a number of security techniques in the cloud. Here we present some of them in detail:

i) *Security and Privacy issues*

A language which is used to allow data with policies by agent is provided by the author of [6] here agent has to prove their action and authorization to use particular data. In this technique the owner of the data attaches policies with data that contain a description of which actions are allowed with which data. But there is the problem of Continuous auditing of agent. But the work has also provided solution which monitors the incorrect behaviour of agent. The agent has to give justification for their action, after that authority will check the justification. A privacy manager mechanism was given by S. Pearson in which the user's data is in encrypted form in cloud and evaluation is done on encrypted data. The privacy manager makes readable data from result of evaluation manager to get the correct result. As in obfuscation data is not present on Service provider's machine so there is no risk with data and hence data is safe on cloud. But this solution is not suitable when input data is large where this method can still require a large amount of memory [4]. The authors of [5] presents mechanism in which policies are decided by the parties that use, store or share the data irrespective of the jurisdiction in which information is processed. But data processed on service provider is in unencrypted at the time of processing so there is a risk of data leakage which becomes disadvantage of this mechanism. There is a method of dynamic auditing protocol proposed by authors in [8] which supports the dynamic operations of the data on the cloud servers, but this method may leak the data content to the auditor as it requires the server to send the linear combinations of data blocks to the auditor. In [10], the authors extended their dynamic auditing scheme to be privacy preserving and support the batch auditing for multiple owners. However, due to the large number of data tags, their auditing protocols may incur a heavy storage overhead on the server. In [7], authors have given a three layer architecture which protects information leakage from cloud; it provides three layers to protect data. In first layer the service provider is not allowed to view confidential data, in second layer service provider should cannot do the indexing of data, in third layer user specify use of his data and indexing in policies. In this way policies always travel with data. In paper [2], the authors propose a novel automatic and enforceable logging mechanism in the cloud. To our

Knowledge, this is the first time a systematic approach to data accountability through the novel usage of JAR files is proposed. Their proposed architecture is platform independent and highly decentralized, in that it does not require any dedicated authentication or storage system in place but here multiple jar files (inner jars), takes lot of time to execute and latency is noticed by data users.

ii) Other techniques

With respect to Java-based techniques for security, our methods are related to self-defending objects (SDO). Self-defending objects are an extension of the object-oriented programming paradigm, where software objects that offer sensitive functions or hold sensitive data are responsible for protecting those functions/data. Similarly, we also extend the concepts of object-oriented programming. The key difference in our implementations is that the authors still

rely on a centralized database to maintain the access records, while the items being protected are held as separate files. In previous work, we provided a Java-based approach to prevent privacy leakage from indexing, which could be integrated with the CIA framework proposed in this work.

In terms of authentication techniques, Appel and Felten proposed the Proof Carrying authentication (PCA) framework. The PCA includes a high order logic language that allows quantification over predicates, and focuses on the access control for web services. While related to ours to the extent that it helps maintaining safe, high performance, mobile code, the PCA's goal is highly different from our research, as it focuses on validating code, rather than monitoring content.

In paper [10], the authors proposed Identity-Based Encryption scheme (IBE). The scheme has chosen cipher text security in the random oracle model assuming an alternative of the computational Die-Hellman problem. This system is based on bilinear maps between groups. The example of such map is Weil pairing on elliptic curves. They have given precise definitions for secure identity based encryption schemes and given several applications for such systems. Using standard techniques from threshold cryptography the PKG in their scheme master-key is being distributed so that this key is never available in a single location. Unlike common threshold systems, the authors showed that robustness for their system's distributed PKG is free.

In addition, our work may look similar to works on secure data provenance but in fact greatly differs from them in terms of goals, techniques, and application domains. Works on data provenance aim to guarantee data integrity by securing the data provenance. They ensure that no one can add or remove entries in the middle of a provenance chain without detection, so that data are correctly delivered to the receiver. Differently, our work is to provide data accountability, to monitor the usage of the data and ensure that any access to the data is tracked. Since it is in a distributed environment, we also log where the data go. However, this is not for verifying data integrity, but rather for auditing whether data receivers use the data following specified policies

3. MECHANISM

Triple DES algorithm performs three iterations of a typical DES algorithm. In its strongest version, it uses a secret key which consists of 168 bits. The key is then divided into three 56-bit keys.

- 1.Encryption using the first secret key
- 2. Decryption using the second secret key.
- 3. Encryption using the third secret key.

The encryption and decryption operations may be presented as Mathematical equations:

Encryption:

$c = E_3(D_2(E_1(m)))$

Decryption:

$m=D_1(E_2(D_3(c)))$

3DES with short keys:

Using DES decryption operation in the second step of 3DES encryption provides backward compatibility with the original DES algorithm. In this case, the first and second secret keys, or the second and the third secret keys should be identical, and their value is not important.

$C=E_3(D_1(E_1(m)))=E_3(m)$

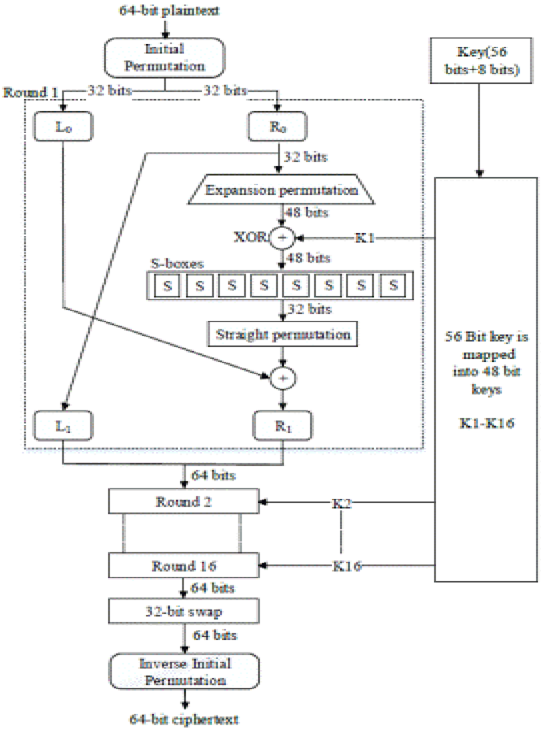
$C=E_3(D_3(E_1(m)))=E_1(m)$

It is also possible to use the 3DES cipher with a secret key of size 112bits.In this case, the first and third secret keys should be identical. Such an approach is stronger than simple DES encryption used twice because it provides better protection against meet-in-the-middle attack.

$C=E_1(D_2(E_1(m)))$

4. SECURITY DISCUSSIONS:

3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56). TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is,[1] the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3 [11]. The standards define three keying options:



Option 1, the preferred option, employs three mutually independent keys (K1 ≠ K2 ≠ K3 ≠ K1). It gives keyspace of 3 × 56 = 168 bits.

Option 2 employs two mutually independent keys and a third key that is the same as the first key (K1 ≠ K2 and K3 = K1). This gives keyspace of 2 × 56= 112 bits.

Option 3 is a key bundle of three identical keys (K1 = K2 = K3). This option is equivalent to DES Algorithm.

In 3-DES the 3-times iteration is applied to increase the encryption level and average time. It is a known fact that 3DES is slower than other block cipher methods [11, 12].

5. CONCLUSION

This paper presents a detailed study of the popular Encryption Algorithm 3DES. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used. Of them 3DES stands to be best as it is capable of withstanding the major attack like meet-in-the-middle attack.So we can say that this paper presented the best to provide information of 3DES. As this algorithm includes 2 encryptions and 1decryption it is not possible for the intruder to hack data of the customers.

Our future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval.

REFERENCES

[1] Gurupreethsingh, Supriya "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security"*International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013*

[2] SmithaSundareswaran, Anna C. Squicciarini and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud,", IEEE Transaction on dependable a secure computing, VOL. 9, NO. 4, pg 556-568, 2012.

[3] B.Crispo and G.Ruffo, "Reasoning about Accountability within Delegation" Proc. Third Int‟ l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001.

[4] S. Pearson, Y. Shen, and M. Mowbray," A privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (cloudcom), pp.90- 106, 2009.

[5] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud, "*Proc First Int'l conf. Cloud* Computing, 2009.

[6] R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.

[7] A. Squicciarini , S. Sundareswaran and D. Lin, " Preventing Information Leakage from Indexing in the Cloud," *Proc. IEEE Int'l* Conf.Cloud Computing, 2010

[8] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li,"Enabling public auditability and data dynamics for storages security incloud computing", inINFOCOM.IEEE,2010,pp. 525-533.

[9] C.Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing,"in INFOCOM. IEEE, 2010, pp. 525–533.

[10] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int‟ l Cryptology Conf.

[11] "3DES", http://www.cryptosys.net/3des.html

[12] "3DES", http://en.wikipedia.org/wiki/Triple_DES

[13] Ajay Kakkar, M. L. Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012.