International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 1
ISSN: 2454-4248
137 – 142

Security of Data with 3DES & Watermarking Algorithm

Swati Singh
M-tech Student
Computer Science, BBAU Central University,
Lucknow, UP, India
Swatisikarwar993@gmail.com

Sarita Soni
Assistant Professor
Computer Science, BBAU Central University,
Lucknow, UP, India
saritasoni90@gmail.com

***Abstract*—** Cloud computing is architecture for providing, pay per use, services on demand of the user over the network. Although cryptography can be used to provide the security of data but it has a problem. This cryptography problem is that, when we convert our plain text into the cipher text then it becomes meaningless, so the intruder will interrupt the transmission on the data from sender to recipient. On the other hand water marking technique is also widely used for the security of data. So in this paper, a merged technique, combination of cryptography and water marking, is proposed to enhance the security of data. Firstly, for hiding the original message Triple Data Encryption Standard (3DES) algorithm will be used. Secondly, the water marking technique will be used over the encrypted message. Therefore, the multiple level securities will be provided using this proposed system.

Keywords: *Cloud Computing, Cloud Architecture, cloud with Cryptography, 3DES, Water Marking Techniques.*

*****

I. INTRODUCTION

Back in past if we had to access a file or document to another computer, we would have to copy the file to an external disc and bring it to the computer on which the file was supposed to be accessed. But now we can access a file on the computers placed miles away from our personal computers without copying it or bringing it in some external drive. This process of copy and paste can be removed by using the cloud storage. We can simply share the files on the cloud and these shared files at can be accessed at any place on the world without any interruption. Cloud computing, on the other hand, also helps in maintaining privacy of our confidential files as the information saved in external drives can be easily accessed by anyone if the drive is lost whereas the clouds are protected with password so none other than you can access the data stored on it. So Cloud computing refers to manipulating, configuring and accessing the applications online. Basically cloud computing offers to many users or businessmen's infrastructure, online data storage and applications over the internet. According to the NIST (National Institute of Standards and Technology), the essential characteristics of cloud computing can be defined as-

1. On-demand self-services
2. Ubiquitous network access
3. Resource pooling
4. Location independence
5. Rapid Elasticity
6. Measured services

II. CLOUD COMPUTING MODELS

For making the cloud computing more feasible and accessible to the end-users, we generally use two services model:

I. Deployment model
II. Service model

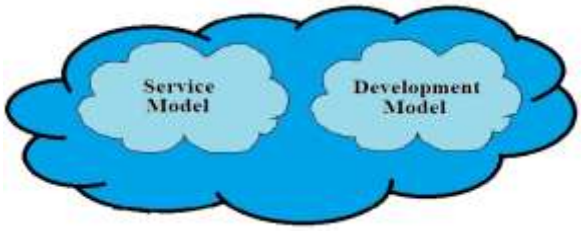

Figure1- Cloud Computing Model

1. Deployment model- Deployment model defines the type of access to the cloud. It can be accessed by four types Public cloud, Private cloud, community cloud and Hybrid cloud.

1.1. Public cloud:
The public cloud allows system and services to be easily accessible to the general public. So this cloud may be less secure because of its openness. E.g., email.

1.2. Private cloud;
As the private cloud is self explanatory. Here, private cloud, system and services are allows to be easily accessible within an organization. The security level is too high because of its private nature.

1.3. Community cloud:
A group of organizations will be allowed to access the system and services in the community cloud.

1.4. Hybrid cloud:
Hybrid cloud can be defined as the combination of public and private cloud, where all the critical activities are performed by the private cloud and public cloud is used to perform the non-critical activities.

2. Service model- Service model can be defined as a reference model on which the cloud computing is based. This can be categorized into three types SAAS, PAAS and IAAS.

 ISSN: 2454-4248
137 – 142

2.1. Software as a service:
Different software applications are provided over the internet by the Application Service Provider (ASP).). SAAS model allows end user to use software applications as a service. With the use of SAAS, user will not have to install various on their own systems [3]. User can access their applications as per their need and pay according to their use. In SAAS, extra load can be avoided and full support system will be provided to the end user. **E.g.,** Google App.

2.2. Platform as a service:
PAAS provide the runtime environment for applications, development and deployment tools. In PAAS, a platform is provided to all the end users as a service without having to download or install software. PAAS also support Web-development interfaces such as simple object access protocol which allows the construction of multiple web services. **E.g.,** Google App Engine.

2.3. Infrastructure as a service:
Where SAAS and PAAS are proving applications to customers IAAS does not. It simply offers the hardware so that the organization can put whatever they want onto it. So, it is beneficial for end users to use those resources provided by the IAAS on rent instead of buying those server and software. The various services provided by the IAAS are-

1.3.1 Server Space
1.3.2 Network equipment
1.3.3 Memory
1.3.4 CPU Cycles
1.3.5 Storage Space

III. CLOUD WITH CRYPTOGRAPHY

Whenever we save our valuable information on our phones and desktops or on our notebooks, we always get worried about the security of data. .The main aim of ours is to save that information from the third party vendor or from the unauthorized user. So security is the major concern which we have to keep in our mind. This is the biggest issue of today's world. To save our data on the cloud we use various techniques and cryptography is one of them. We use various cryptography algorithms to keep our data more secure from the unauthorized access. Whenever we have to send our data from one network to another network over the internet, there are so many possibilities to get our data leaked by the third party. So while sending our data to the destination from the source we simply perform two operations the first one is encryption and another one is decryption. Encryption is also used to protect our data and plays a vital role for the security of data. Encryption can be defined as a technique of securing our data from the intruders in which a plain text is converted into the cipher text and cannot be readable by them. So we apply the encryption technique over the data which we have to send using a private key and send that data to its destination over the network. On the other hand the desired party gets the data and applies the decryption technique using the public key provided by the user. So basically by using these techniques we can save our data from the unauthorized users and also safe from the outsiders. This is the best way to secure our data from the intruders by encrypting our data from original to non-readable form. The reverse of this process is known as the cryptanalysis process in which the non-readable data is converted into in its original form without knowing how they were initially converted from readable to non-readable format. On the other hand, the combination of both cryptography and cryptanalysis is known as the cryptology.

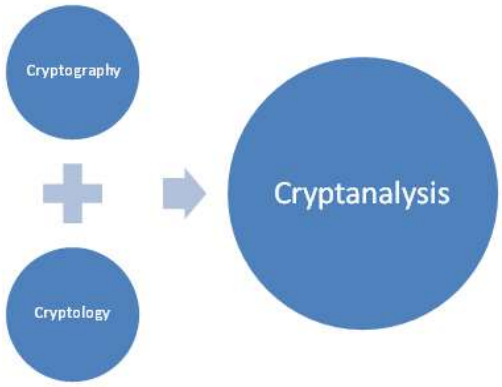

Figure2- Cryptography

IV. EXISTING SYSTEM

In cryptography, there are many algorithms which are used for the security of data. Cryptography can be basically divided into two parts. One of them is symmetric cryptography and another one is asymmetric cryptography. In symmetric cryptography we only use one key for both encryption and decryption process. The algorithms used in symmetric key cryptography are AES, DES, and 3DES. On the other hand asymmetric key cryptography we use two keys one for he encryption and one for the decryption process. By using the asymmetric cryptography we can provide the authentication and non-repudiation. The algorithms used in asymmetric key cryptography are RSA and Elliptic Curve Cryptography.

1. 3DES

3DES is developed by IBM in 1978. It is the successor of DES algorithm which uses 168 bits key size. The key size of 3DES algorithm is 3 times bigger than the key size of DES algorithm i.e., (3*56 bits) and the block size of 3DES algorithm is 64 bits. 48 rounds are used in 3DES algorithm for the encryption process. There are three main steps are in the 3DES algorithm and which are as follows:

1.1 Encryption process is done with a key K1.
1.2 Decryption process is done with a key K2.
1.3 Encryption process is done with a key K1.

 ISSN: 2454-4248
137 – 142

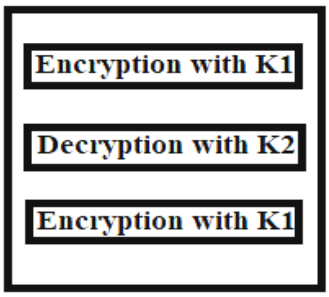

Figure3- Steps In 3DES Algorithm

Advantages of 3DES:

1. Implementation is easy in hardware and software.
2. Increases the level of encryption, so security will be enhance exponentially.

Disadvantages of 3DES:

1. Due to increase in rounds its performance becomes poor.
2. In comparison with other cipher methods, it is quite slow.

2. RSA

RSA algorithm is introduced by Rivest, Shamir and Adelman in 1978. RSA algorithm is an example of asymmetric key cryptography in which two keys are used. One key is used for encryption process. This key is also called the private key which is known only to the end user. The second key is used for decryption process which is called public key and it is known to all. In the RSA algorithm, the key size is (>1024bits) and the block size is minimum 512 bits.

RSA algorithm involves these steps:

1. Key Generation

2. Encryption

3. Decryption

Algorithm

Following algorithm is used in RSA,

1. Choose p and q
2. Compute n = p * q
3. Compute φ(n) = (p - 1) * (q - 1)
4. Choose e such that 1 < e <φ (n) and e and n are co-prime.
5. Compute a value for d such that (d * e) % φ (n) =1.
6. Public key is (e, n)
7. Private key is (d, n)
8. For encryption C=me (mod n) and decryption m =cd (mod n)

Hence, by following above algorithm the plain text in encrypted form or cipher text and then decrypted from cipher text to plain text.

Advantages of RSA:

1. RSA algorithm uses two keys for encryption and decryption process.
2. Security gets maintained at high level because there is no need to transmit the private key.
3. As the key size of RSA algorithm is >1024 bits, so the code length will be maximum.

Disadvantages of RSA:

1. Speed is the biggest disadvantage of RSA algorithm. It provides very slow processing.

3. DES

DES stands for data encryption standards which is developed in 1977.DES was approved by the National Bureau Of Standards (NBS), now called *National* Institute of Standards and Technology (NIST). DES completes the 16 rounds of encryption on each 64 bits block of data. DES is an example of symmetric key cryptography in which a single key is used for both encryption and decryption process. In DES algorithm, DES accepts an input of 64 bit long plain text and generates the output of 64 bit block. The key size of DES algorithm is 56 bits and the block size is 62 bits.

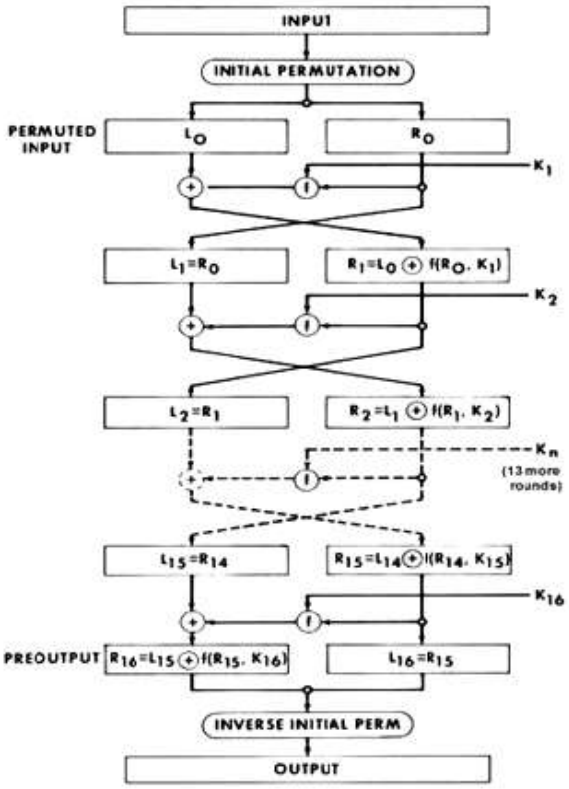

Figure4- DES algorithm

 ISSN: 2454-4248
137 – 142

Advantages of DES:

1. DES is used in many commercial and financial applications.
2. DES has proved resistant to all forms of cryptanalysis.

Disadvantages of DES:

1. Due to the advancement in computer processing power it was recognized that DES was not secure.
2. The key size of DES algorithm is too small by current standards.

4. AES

Advanced Encryption Standard (AES) was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen in 2001. AES algorithm is not only used for security but also for the great speed. In Advanced Encryption Standard, Both hardware and software implementation are faster still. Advanced encryption standard, recommended by NIST to replace DES, is a successor of DES. AES Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size. AES is an example of symmetric key cryptography in which a single key is used for both encryption and decryption process.

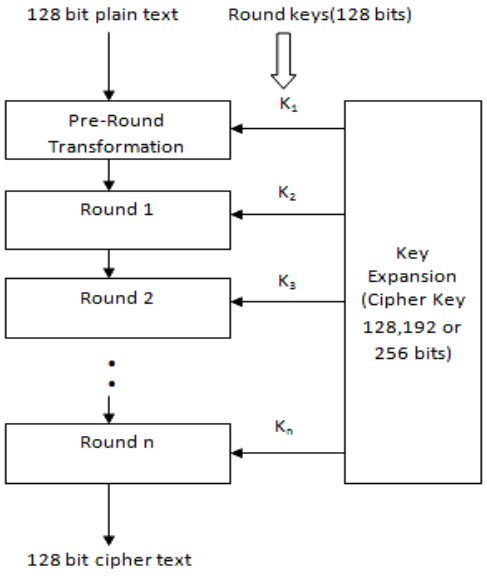

Figure5- AES Algorithm

Advantages of AES:

1. AES algorithm is used to replace the less reliable algorithms, such as Data Encryption Standard (DES).
2. AES encryption is fast and flexible.
3. The key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information.

Disadvantages of AES:

1. Sometimes it becomes complex due to its too long size of key length.

V. PROPOSED SYSTEM

Nowadays security is the main concern because our data gets easily accessed by the cyber criminals. In the cloud various recourses are available in order to provide the facilities to the end users. So, Authentication and Integrity of stored data is a necessary for the secure communication.

Design and Algorithm:

The proposed system uses the hybrid algorithms (3DES and Watermarking) for the better security of data. This system is only designed to maintain the security of text files. In the proposed system 3DES and Watermarking technique is used for the encryption of text files and on the other side the inverse 3DES and Watermarking is used for the decryption of text files when it is downloaded by the user.

A. For the Encryption Process of Data:

1. Upload the text file.
2. Implement the Watermark to generate the first level of authentication.
3. Implementing 3DES algorithm to generate the first level of encryption using key K1.
4. Implementing 3DES algorithm to generate the second level of decryption using key K2.
5. Implementing 3DES algorithm to generate the third level of encryption using key K1.
6. Implement the same Watermark to generate the second level of authentication.

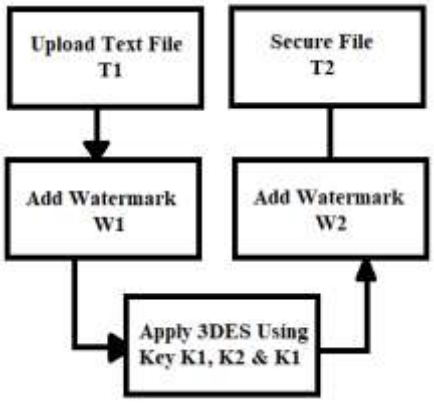

Figure6- Block diagram of multilevel encryption

As shown in the figure 2, the steps of multilevel encryption are as follows:

 ISSN: 2454-4248
137 – 142

- Upload the text file T1.
- Now in the second round a watermark is implemented for the authentication of uploaded data T1. Watermarks are used for the security of data. Watermark is nothing just a symbol which is added with the content for the security. It also helps in finding out the data which is hacked by the third parties.
- After implementing the watermark on the data, implementation of 3DES takes place. Triple DES is the mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. 3DES uses 48 rounds. As the number of rounds increases the security is also increases exponentially. So in this step the data will be encrypted by using a key K1.
- Again we implement the 3DES algorithm for the decryption process of data which is encrypted at the first level. For the decryption of data we use the key K2
- In the next step another encryption process is done by using the 3DES algorithm by using the key K3.
- Finally at the end of the 3DES algorithm another implementation of watermark takes place. This watermark will be different as the watermark added in the first level.

B. For the Decryption Process of Data:

1. Read the cipher text T2 from the database.
2. Remove watermark W2 if it is authenticated.
3. Implementing 3DES algorithm to generate the first level of decryption using key K1.
4. Implementing 3DES algorithm to generate the third level of encryption using key K2.
5. Implementing 3DES algorithm to generate the fifth level of decryption using key K1.
6. Remove watermark W1 if it is authenticated.

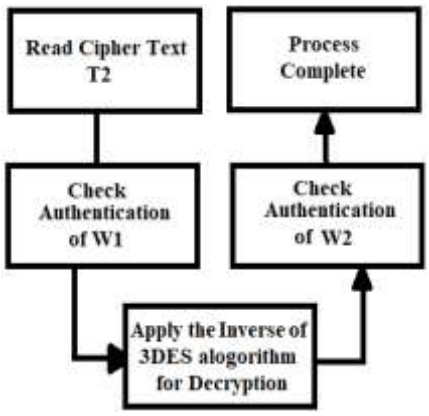

Figure7- Block diagram of multilevel decryption

As shown in the figure 3, the steps of multilevel decryption are as follows:

- Read the uploaded cipher text of the text file T2.
- Now in the second round the implemented watermark will be checked for the authentication of uploaded data T2. If this watermark will be authenticated then it will be removed and further process will take place.
- After removing the watermark from the data, implementation of 3DES takes place. So in this step the data will be decrypted by using a key K1.
- Again we implement the 3DES algorithm for the encryption process of data which is decrypted at the first level. For the encryption of data we use the key K2
- In the next step another decryption process is done by using the 3DES algorithm with the key K1.
- Finally at the end of the 3DES algorithm another watermark will be checked for the authentication. Watermark will be removed if it is authenticated.

IV. RELATERD WORK

1. Singh et.al. [1] Studied various encryption algorithms in their research work. In cryptography various algorithms are used for the security purpose and these algorithms are AES, DES, RSA and 3DES. These various algorithms are compared based on the several factors such as key length, rounds, cipher text, speed and security. In this comparison they calculated that RSA has the smallest speed of encryption and decryption. But the AES has the finest speed of encryption and decryption. So, in this paper, they concluded that AES is the best technique for the security of data.

2. Jaatun et.al. [2] Implemented an algorithm on confidentiality for cloud computing. Their research was based on the redundant array of independent net-storages (RAIN) for cloud computing. In RAIN approach the data stored on the cloud gets divided into segments and then gets distributes. If the relation between the distributed segments is private then it prevents the reassembly of the original data. As the size of each segment is too small so that it cannot be able disclose any meaningful and useful information to the unauthorized user. So, in this paper, by using the RAIN approach the confidentiality of data can be ensured that is stored in the cloud.

3. Chakraborty et.al. [3] Represented a brilliant idea of elliptic curve cryptography for a hemimorphy encryption scheme. They have used the notion because notion is important for the proposals in the cryptography. So here the notion was

 ISSN: 2454-4248
137 – 142

used for the verification and the modific3tion of secured path data on behalf of the client. They used the merkle hash tree for the data server storage.

4. Randeep Kaur et.al. [4] Mentions some of the notable challenges associated with cloud Storage. The challenges are Security, Privacy and Lack of Standards which slow down services in the cloud.

5. Mrinal Kanti Sarkar et.al [5] enhances data storage security in cloud computing through Steganography. By this technique the integrity of data will be maintained at higher level. In this technique the original data is hidden behind the images so that the un\authorized users will not be able to interrupt the data.

CONCLUSION

Cloud computing can be defined as a set of services and resources which are offered to an end user over the internet by the cloud vendors. The services provided by the cloud vendors are useful in the secure storage of data from the unauthorized user. As we know that many cryptographic algorithms are used for security of data but in this paper we used the multiple levels to secure the data. So if our information can be accidently retrieved by the unauthorized user then it will be very difficult to decode the data due to multilevel of encryption. This hybrid technology will provide the higher level of security than the single level of encryption.

REFERENCES

[1]. Singh, Gurpreet, and A. Supriya. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", IJCA 67.19,pp-33-38, 2013.
[2]. M. G. Jaatun, A. A. Nyre, S. Alapnes, and G. Zhao, "A farewell to trust: An approach to confidentiality control in the Cloud." pp. 1-5.
[3]. T. K. Chakraborty, A. Dhami, P. Bansal, and T. Singh, "Enhanced public auditability & secure data storage in cloud computing." pp. 101-105.
[4]. Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847),Volume 3 Issue 3, pp.171-176, March 2014.
[5]. Enhancing Data Storage Security in Cloud Computing Through Steganography by Mrinal Kanti Sarkar and Trijit Chatterjee in ACEEE Int. J. on Network Security, Vol. 5, No. 1, January 2014.
[6]. Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", / International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4, pp.1922-1926, Jul-Aug 2013.
[7]. Shakeeba S. Khan, Prof.R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering, volume-3, pp-143-154, January 2015.
[8]. Mrunalini Motilal Shete, Pragati Damodar Hipparkar, "Data Secure in Cloud Computing Using Encryption Algorithms ", International Journal of Science and research (IJSR), Volume 4 Issue 3, pp- 1497-1499, March 2015.
[9]. Rohit Bore, Dr. Rahila Sheikh, "International Journal of Computer Science and Network", Volume 5, pp-171-176, February 2016.
[10]. Dr. S. S. Manikandasaran, "Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage", International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol.6, pp- 498-503, Jan-Feb 2016.