ISSN:0975-9646

Garima Saini et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5825-5827

# Triple Security of Data in Cloud Computing

Garima Saini
*Mtech Scholar*
*Gurgaon Institute of Technology and Management*
*Bilaspur , Gurgaon*

Naveen Sharma
*Assistant Professor*
*Gurgaon Institute of Technology and Management*
*Bilaspur , Gurgaon*

**Abstract—cloud computing is the biggest buzz in computer world now a days. It is providing excellent facilities by flexible infrastructure. Cloud computing is based on client-server architecture . cloud computing is a hub of various server and many database to store data. cloud computing provide many services to user which is reliable , efficient and low cost. As it is internet based technology security , data security becomes a big issue to the cloud data. Many issues like data authenticity , integrity , data hiding and availability. In this paper we introduce a mechanism to provide secure data. We combine three algorithm DSA , DES and Steganography to provide security of data in cloud computing.**

**Index Terms— Cloud computing , DSA , DES , Steganography .**

## I. INTRODUCTION

Cloud computing is a term which is used to refer a model of network computing where a program or application runs on a connected server or servers rather than on a local computing device such as a PC, like the traditional client server model. Cloud computing relies on sharing of resources to achieve coherence of network. Cloud computing have aimed to allow access large amounts of data in a fully virtualized manner. Cloud computing allows for the sharing and scalable deployment of services from almost any location, for which the customer can be charged based on actual usage .Security is needed against unauthorized access and to reduce risks of data stealing. Cloud provider hosting a large set of databases to their customer and by securing cloud means that storage should be protected and secured for the privacy purpose. In this paper we will focus the security of data in cloud computing – how data is to be secure on cloud.

## II. SECURITY IN CLOUD COMPUTING

Cloud computing provide several services to their clients. cloud computing is a huge collection of inter connected network. So main challenge is to provide security to cloud network . There is number of security concern associated with cloud computing. The main aim of security is to provide availability, confidentiality, integrity to the data. There are so many risk associated with the cloud network like data can be hacked by an unauthorized person. Data can be changed by third party while transferring the data. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths . In this paper we will use 'Triple Security in Cloud Computing' by using three different security algorithms such as-

1) DSA (Digital signature algorithm)
2) DES (Advanced Encryption Standard)
3) Steganography – hiding data behind an audio file.

## III. METHODS OF SECURITY IN CLOUD COMPUTING

### *A. DSA(Digital Signature Algorithm)*

Digital signatures are very essential in modern world to verify the sender's identity. Digital signature is an electronic signature which is used for verification and authentication of data. A digital signature is represented as a string of binary digits in computer system. The signature is using a set of rules and parameters (algorithm) such that the identity of the person signing the document as well as the originality of the data can be verified. The signature is generated with the help of a private key. A private key is known only to the sender. The signature is verified by receiver by use of a public key which corresponds to the private key. Digital signature can be used with any kind of data whether it is encrypted or not. Digital signatures are used to detect unauthorized modifications of data by third party. Also, the recipients of a digitally signed document assure that the document was indeed signed by the person who it is claimed to be signed by. This is known as nonrepudiation, because the person who signed the document cannot repudiate the signature later . Digital signature algorithms can be used in e-mails, electronic funds transfer, software distribution, data storage that assure the integrity , authenticity and originality of data. A hash function is used in the signature generation process to obtain a condensed version of data, called a message digest. The message digest is then input to the digital signature algorithm to generate the digital signature.

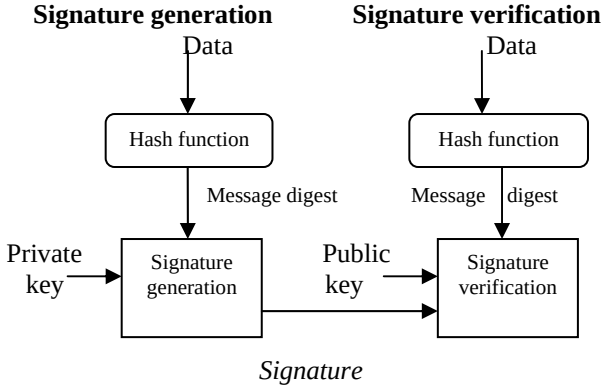


Figure – 1 Digital Signature Scheme

*B. DES(Data Encryption Standard )*

DES was designed by IBM in 1970 and adopted by the U.S.govt.as the standard encryption method. DES is widely used method for encryption of data. DES is block cipher which use shared secret key. It is based on symmetric key algorithm which uses 56-bit key and 64-bit block of data. Eight bit is consider as a parity bit. The process of DES involves 16 rounds and in each round certain operation like substitution and permutation is performed between text which is to be encrypted and key. During DES encryption following processes is done

- Partitioning of text into 8 block each of 8-bit.
- Initial permutation(IP)
- Breakdown of text into left half and right half
- Permutation and Substitution
- Inverse Permutation

Firstly each bit of block is subjected to Initial permutation(IP) .Once IP is completed input text is divided into two part left half(32) and right half(32). Then right half is expanded to 48 bit. This process is called expansion permutation. After E-permutation 48-bit key is xored with 48 bit Rightmost half. After Xor operation, the block is divided into eight 6-bit pieces before processing by the S-box computation. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation. S-box provide core of security in DES. Finally, the 32 outputs from the S-boxes are rearranged according to a fixed Permutation. The alternation of substitution from the S-boxes, and permutation of bits from the P-box and E-expansion called confusion and diffusion.

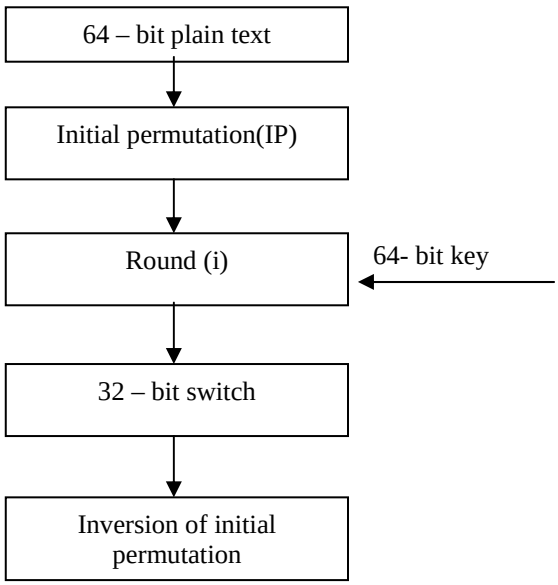


Figure – 2 DES Scheme

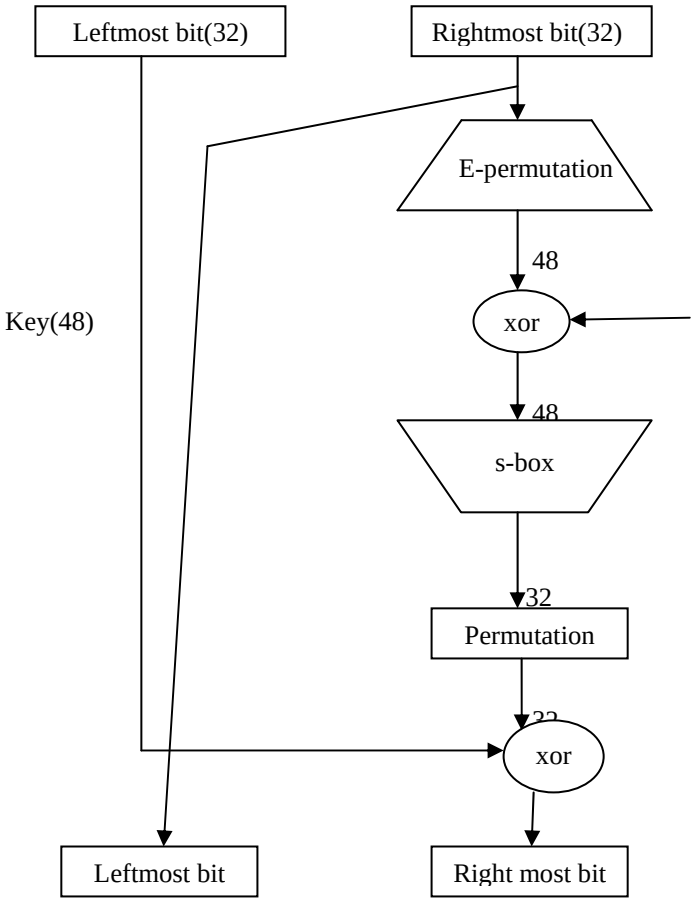


Figure – 3 Flow diagram of one round

*C. AES(Advanced Encryption Standard)*

After DES was used as an encryption standard for over 20 years and it was able to be cracked in a relative short amount of time, NIST decided a new standard, the Advanced Encryption Standard (AES), needed to be put into place. AES is based on Rijndael cipher.AES has been adopted by US government and is widely used now a days. This decision was announced in January 1997, and a request for AES candidates was made. The AES was to be a symmetric block cipher algorithm supporting keys sizes of 128-, 192-, and 256-bit keys. AES is based on substitution and permutation network. It does not use Feistel network. It is more secure than DES and hard to crack. AES is more complex than DES but it is fast and very efficient. It work with 128 bit fix block size plain text and variant key sizes.

D. STEGANOGRAPHY

Steganography is the art and science of hiding a messages in such a way that no one apart from the intended recipient knows of the existence of the message. Steganography is the process of hiding one medium of communication (text, sound or image) within another. The word Steganography comes from the Greek steganos (covered or secret) and graphy (writing or drawing) and so it literally means, covered writing. Steganography is the practice of encoding secret information in a manner such that the very existence of the information is concealed under the image or picture

where it is hided. Throughout history, many steganography techniques have been documented, including the use of cleverly-chosen words, invisible ink written between lines, modulation of line or word spacing, and microdots. Usually the secret information is concealed by the use of an innocuous cover so as to arouse no suspicion to anyone. As an example, the cover text: "I'm feeling really stuffy. Emily's medicine wasn't strong enough without another febrifuge. Advantage of steganography over cryptography is that secret message does not attract attention to itself as message can be concealed under image file , video file etc.

There are different technique of steganography :

1) Data concealing within wax tablet.
2) Data concealing within noisy image.
3) Hidden messages under blank part of another message.
4) Data hiding within audio file.
5) Data hiding under video file.

## IV. OVERALL DESIGN OF PROPOSED WORK

In our proposed work we provide security by implementing three algorithm DSA , DES and steganography together to cloud network. To implement these three algorithm we use Asp.net as a platform.

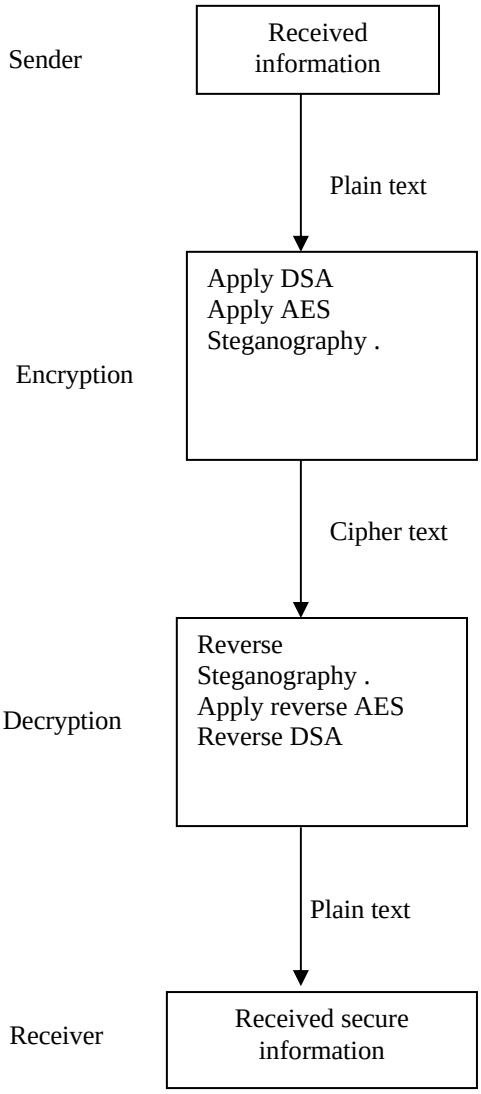


Figure – 4 Overall system design

In our proposed system for encryption first apply DSA for authentication of data. Then apply AES algorithm for encryption and then hiding data within audio file for provide maximum security to the data. Receiver can get original plain text by reversing the stegnography , AES and DSA .

## V. CONCLUSION AND FUTURE WORK

In this paper we implements Digital signature Algorithm, Data Encryption Standard and Steganography to provide maximum security in cloud computing. By implementing these three algorithm we provide authenticity , security and data integrity to tha data. We find that the Time complexity is high because it is a one by one process but in future this time complexity could be reduced. We try to improve the time complexity by using other security algorithms.

## REFERENCES

[1] Chao Yang, "A novel triple Encryption Scheme for Hadoop based cloud computing", in Emerging intelligent data and web technologies , IEEE , Sep- 2013.

[2] Patidar , S "Survey on cloud computing" , in Advanced computing and communication technologies , IEEE , Jan- 2012..

[3] M. Vijayapriya, "Security algorithm In Cloud Computing: Overview"/ International Journal of Computer Science & Engineering Technology(IJCSET)

[4] Rashmi Nigoti, Manoj Jhuria & Dr. Shailendra Singh," A Survey of Cryptographic algorithms for Cloud Computing.In International Journal of Emerging Technologies in Computational and Applied Sciences(IJETCAS), ISSN(print) 2279-0047, ISSN(online):2279-0055.

[5] B.Arun & S,K. Prashanth, " Cloud Computing Security Using Secret Sharing Algorithm" in Indian Journal of Research, ISSN-2250-1991, Volume:2|Issue: 3| March 2013.

[6] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan & Bhavani Thuraisingham, "Security Issues for Cloud Computing" in International
Journal of Information Security and Privacy, 4(2),39-51, April-June 2010.

[7] Ew Approach to Hide Text in Images Using Steganography" in International Journal of advanced Research in Computer Science and software Engineering, ISSN:2277 128X, Volume 3, Issue 4, April 2013.

[8] V.K. Zadiraka & A. M. Kudin, " Cloud Computing In Cryptography And Steganography", in Cybermetics and Systems Analysis, Vol. 49, No. 4, July-2013, UDC 681,3;519,72;003,.26.