International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 1007 – 1009

Triple Security in Cloud Computing

Aakansha Sharma[1], Dr. Sachin Gupta[2]
Computer Science and Engineering Department , MVN University, India
Sharma.aakansha90@gmail.com
Sachin.gupta@mvn.edu.in

Abstract **–**The word Cloud stands for Common Location & Independent Online Utility as per demand. It is the growing technology in today's IT industries. Companies like Google, Amazon, Microsoft either small or large scale industries needed cloud technology as it is providing virtualized environment which omits the need for physical storage. Cloud Computing is type of computing which relies on sharing computing resources instead of having local servers to handle applications. As this is Internet based technology, here data security becomes major issue for cloud data. In this paper we introduce a mechanism for providing secure data using three algorithms DSA, DES and Steganography.

Keywords- *Cloud Computing, DSA, DES, Steganography.*

*****

I. INTRODUCTION

In Cloud Computing we deploy groups of remote servers and software network who allow different kind of data to be uploaded for real time processing which produce computing result without the need to store processed data on the cloud. Cloud Computing is the concept of "ON-DEMAND" access of data in a fully "VIRTUALIZED" manner. So in this type of "Internet based Computing" security is needed against unauthorized access and also we need to do something to reduce the risk of data stealing. In this paper we will focus on the security of data in Cloud Computing. Cloud Computing has three service models which are Public, Private & Hybrid.

II. SECURITY IN CLOUD COMPUTING

Security in Cloud Computing include control based policies and technologies which are designed to regulate compliance rules and protect infrastructure, applications and information which is associated with use of cloud computing. The main aim of cloud computing security is to provide data availability, integrity and confidentiality. As there are many risk associated with the cloud network like hacking of data from an unauthorized person. Data can also be manipulated or changed by third party while we are transferring data on cloud. Cryptography is one of the effective way of protecting sensitive information's which is stored on media transmitted through cloud. In this paper we will perform "Triple Security in Cloud Computing" by applying three different security algorithms as:

1) Digital Signature Algorithm(DSA)
2) Data Encryption Standard(DES)
3) Steganography

Figure 1.1: Generic Structure of a Cloud Computing Security

III. PROPOSED SOLUTIONS FOR CLOUD COMPUTING SECURITY

A. DIGITAL SIGNATURE ALGORITHM (DSA)

In Today's world Digital Signature Algorithm is very much required to verify the sender's identity. Digital Signature is actually an electronic signature which is used for authentication and verification of data. So Digital Signature Algorithm basically authenticates the integrity of the signed data and the identity of the person who actually signed it. The Digital Signature Standard(DSS) uses three algorithms for digital signature generation and verification.

a) Digital Signature Algorithm(DSA)
b) Elliptic Curve Digital Signature Algorithm defined in ANSI X9.62
c) RSA Digital Signature Algorithm defined in ANSI X9.31

A Digital Signature is represented in computer as a string of binary digits. In DSA signature generation makes use of Private Key to generate digital signature whereas signature verification makes use of a Public Key which corresponds to

 ISSN: 2321-8169
1007 – 1009

but is not as same as Private Key. Each user have a Private & Public Key pair, where public keys are known to public but private key are never shared. A Hash function is used in Generation of Signature by which we can obtain Message Digest which is condensed version of data. Message Digest is actually the input to DSA to generate digital signature. The signature is then sent to verifier along with message who verifies signature by using sender's public key.

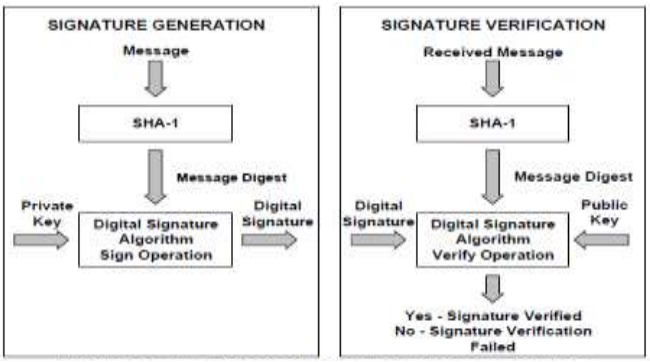

Figure 1.2: Digital Signature Scheme

B. .DIGITAL ENCYPTION STANDARD (DES)

DES was designed by IBM and adopted by the US Government as the Standard Encryption Method. The DES is a block cipher that use shared secret encryption and make use of only a single key. It is based on symmetric key algorithm which uses 64-bit block of data and 56-bit key. Where 8-bit is considered as a parity bit. The process of DES includes 16 rounds and in each round certain operations are performed between text to be encrypted and the key.

- Division of text into 8-blocks of each 8-bit
- Initial Permutation
- Breakdown of text into left and right half
- Permutation and Substitution
- Inverse Permutation

$$IP^{-1} \circ f_{K_2} \circ SW \circ f_{K_1} \circ IP$$

or

$$\text{Ciphertext} = IP^{-1}\left(f_{K_2}(SW(f_{K_1}(IP(\text{plaintext}))))\right)$$

Where

$$K_1 = P8(Shift(P10(key)))$$

$$K_2 = P8(Shift(Shift(P10(key))))$$

Decryption is the reverse of encryption:

$$\text{Plaintext} = IP^{-1}\left(f_{K_1}(SW(f_{K_2}(IP(ciphertext))))\right)$$

We now examine S-DES in more details

Figure 1.3: DES Key Generation

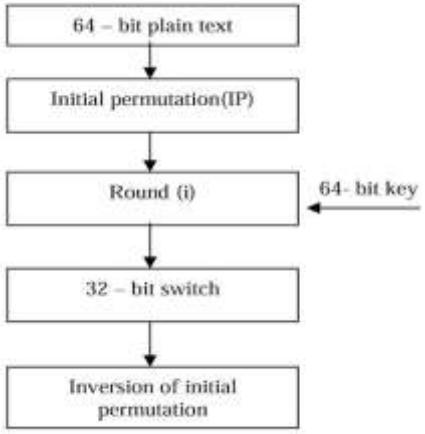

Figure 1.4: DES Scheme

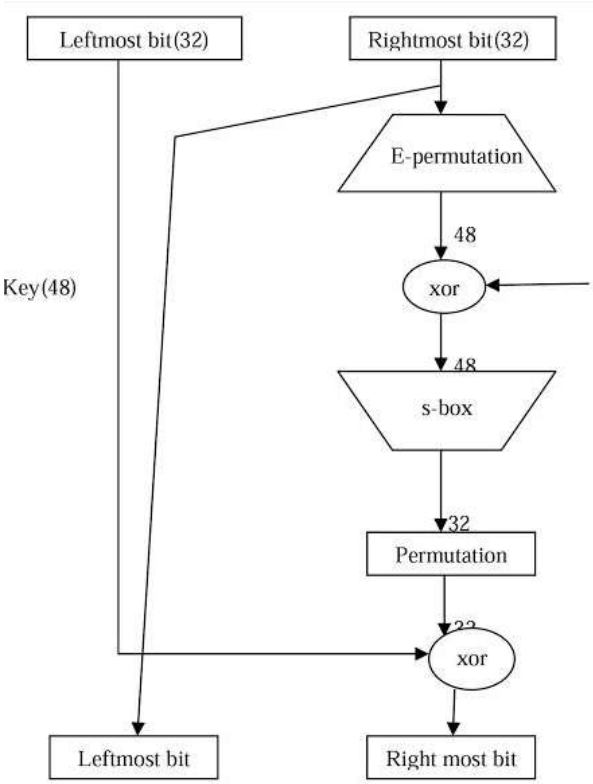

Figure 1.5: Flow Diagram of one round

C. STEGANOGRAPHY

The method of hiding a message in such a manner that nobody apart from the intended recipient knows about the existence of that message is called as Steganography. In Steganography one medium of communication(text, image or sound) is hidden within another medium. This word Steganography is came from Greek where "Steganos" means secret or covered and "Grapgy" means drawing or writing. So combine meaning of Steganograpgy is covered writing. Types of Steganography are:

- Digital Steganograpgy
- Audio Steganography

Different techniques of Steganography are:

- Data concealing within wax tablet
- Data hiding within audio files
- Data concealing within noisy image
- Data hiding under video files
- Hidden message under blank portion of another message

IV. OVERALL SYSTEM DESIGN

The work proposed by us provide security by implementing three algorithms DSA, DES & Steganography. To implement these three algorithm we use Asp.net as platform.

a. DSA-Electronic signature can prove the authenticity of Alice as the original sender of the message.
b. DES-DES was designed by IBM and was adopted by US Government.
c. Steganography- It is actually the art and science of writing a hidden message.

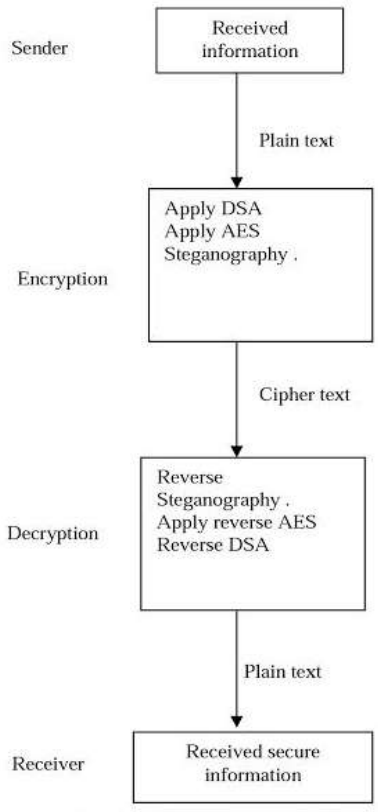

Figure 1.6: Overall System Design

V. CONCLUSION AND FUTURE DIRECTIONS

In this paper we implemented DSA, DES and Steganography to provide maximum security in cloud computing by which means of providing authenticity, security and data integrity to the data.. A cloud service provider must attempt to allow legitimate network traffic and drop malicious network traffic, just as any other Internet- connected organization does. However, unlike many other organizations, a cloud service provider will not necessarily know what network traffic its consumers plan to send and receive. Nevertheless, consumers should expect certain external network perimeter safety measures from their cloud providers. Because it is a one by one process we find that the Time complexity is high but in future we will try to improve the time complexity by using other security algorithms.

REFERENCES

[1] Abdalla,M., Reyzin,L.: A New Forward-Secure Digital Signature Scheme. In: ASIACRYPT 2000,LNCS, Vol.1976, pp. 116-129. Springer-Verlag,(2000).
[2] AN EFFICIENT IMPLEMENTATION OF THE DIGITAL SIGNATURE ALGORITHM P. Kitsos, N. Sklavos
[3] An Introduction to Cryptography and Digital Signatures Author: Ian Curry March 2001 Version 2.0 M.M. Amin, .M. Salleh, S. Ibrahim, M.R Katmin (2003), "Information Hiding Using Steganography", 4th National Conference on Telecommunication Technology Proceeding 2003 (NCTT2003), Concorde Hotel, Shah Alam, Selangor, 14-15 January 2003.
[4] National Institute of Standards and Technology (NIST), Digital Signature Standard, FIPS PUB 186-2, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf
[5] Bellare,M., Miner,S.: A Forward-Secure Digital Signature Scheme. In: Wiener, M. (eds.):