Study of Security Algorithm to Provide Triple Security in Cloud Computing

Khushboo Gupta*, Neha Goyal, Puneet Rani*****

* Department of Computer Science & Engineering
Shri Ram College Of Engineering & Management, Palwal, Haryana, INDIA
*** Asstt. Prof. Shri Ram College of Engineering & Management, Plawal, Haryana, INDIA

Abstract- Among the various technologies of web Cloud Computing is one of the recent internet based computing technology. It provide us a virtual server and a huge size of database to store our data over the internet. Since it is easy to store and manage the data many organizations moving their confidential data into the cloud. But as it is an internet based technology we are concerning about the security related issues like hacking, stealing, misusing etc. These security related issues are the greatest obstacle in the popularity of cloud. Therefore we are going to use the combinations of three different algorithms- DSA, DES and Steganograohy. These algorithms help to reduce the problems of security on cloud.

Index Terms- DES, DSA, Security issues in cloud, and Stagenography.

I. INTRODUCTION

Cloud computing is a modern technology offered through the Internet. Cloud computing is an Internet based computing which provide servers, storage applications and resources to many organizations. There are virtual servers hosting to customers on a pay – as – you – use basis. Cloud computing have aimed to allow access to large amounts of computing power in a fully virtualized manner.[1] This provide an easy and fast access to applications and is also useful to reduce the infrastructure costs. Many companies using cloud computing for their business processes as they only need to pay only for those resources that the use, they do not need their own physical infrastructure. As this new world is totally dependent on internet, people shares, sends and receives their data, information, messages etc. so there is a great need of security for the massive amount of data. 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 in cloud computing – how can data be secure on cloud.

II. SECURITY ISSUES IN CLOUD COMPUTING

The tremendous growth of cloud computing in the variety of organizations may leads to criminal offences, it is important that cloud should also provide security to them. Security in cloud computing is very necessary so that it would be more effective and useful. The users do not have any idea where their data is placed. Since user's data is placed somewhere on the cloud so there might be possibility that a third party who is looking after that stored data. Some illegal activities can harm the data and this is called 'cyber crime'. The next security issue in cloud is that it has a single point of failure. Since cloud is a name given to a group and this is not only for single user but it is for the many users so one mistake or failure can impact the whole group. The other issue related to its security is that the hacker not only hack the cloud data but can also hack the user account. The main aim of security is to provide availability, confidentiality, integrity to the data. [3] 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 (Data Encryption Standard)
3) Steganography – hiding data behind an audio file.

III. ALGORITHMS USED IN SECURITY OF CLOUD COMPUTING

A. DSA(Digital Signature Algorithm):

the digital signature is analogous to the hand written signature. It is used for the authenticity of the document. Similarly, digital signature makes receiver belief that the sender is genuine and the receiving document is authentic. It must verify the author, date and time of the signature. After signing a message, the person cannot deny it. For signing a document 'private key' is used and 'public key' is generated for the signature verification. These keys- private and public are used for confidentiality.
The process of signature algorithm could be understood by the given figure. It shows how DSA works to generate and verified the signature.

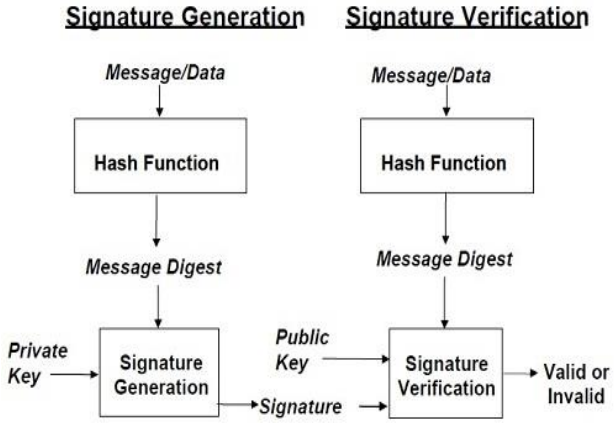

Figure -1 Digital Signature Scheme

In digital signature, the private and public keys of sender are used. The sender uses their private key and the receiver uses the private key of the sender. For encryption receiver's public key is used by sender and receiver uses his own private key to decrypt. Since the message are very long, it is not easy to sign a whole document itself in this case we sign a digest of the message. A secure hash function is used to create message digest- a condensed version of data. Now the signature got verified by the receiver.

B. DES(Digital Encryption Standard)

In cryptography DES is a symmetric key algorithm which have the same key for encryption as well as for decryption. In this technique the users shared a single key. The key is kept secret and therefore it is also called as secret key algorithm. The DES is a block cipher that uses shared secret encryption. The DES can also be used for single – user encryption, such as to store files on a hard disk in encrypted form.[5]

The two main techniques used in DES are XOR operations and numerous permutations. It consists of 64 bit plaintext and 64 bit key but uses 56 bit key during execution. During DES encryption following processes is done

- Initial permutation(IP)
- Key dependence Computation
- Inverse initial permutation

The encryption process is made of two permutations (P- boxes) which we call initial and final permutations and sixteen Fiestel round. Each round uses a different 48 bit round key generated from cipher key according to a predefined algorithm. Decryption is the inverse of DES encryption.[15]

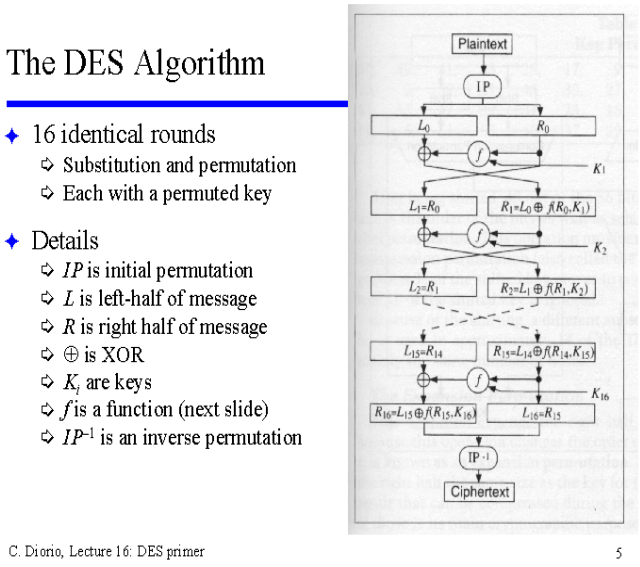

Figure –2 DES algorithm Structure

IV. STEGANOGRAPHY

Steganography is defined as the art and science of writing hidden messages in such a way that no one else apart from the intended recipient knows the existence of the message.[7] It is a technology in network security to hide the message behind an audio, text, object and image. The message could only be read by sender and receiver. It **protects** the message from the third person (hacker) or from unauthorized access. Steaganography term is dissimilar to the cryptography. In cryptography the hacker could recognize the encrypted data by decrypting it using different decrypting methods but this could not be happen in steganography where data is hidden behind a file. The hacker find it a useless data for himself. Fragile and robust are two types of steganography.

There are different methods used in steganography are such as:

i. Hiding messages behind text file.
ii. Hiding messages behind an image.
iii. Hiding messages behind an audio file.
Hiding messages behind video file.

In this paper we are using the method iii. With the tremendous advancement in digital signal processing use of internet computing power, steganography has gone digital.[9]

V. PROPOSED WORK

In our proposed work we are going to reduce the security threats on cloud. In this the three algorithms DSA, DES and staeganography(hiding data behind an audio file) is used together. To implement these algorithms we use .net framework as a platform. The software requirements for the implementation are:

- Microsoft Visual studio 2008
- Windows XP operating System
- MS- Office

The hardware requirements are:

- One computer with 2 GB of memory
- 80 GB hard disk space
- An Intel Premium Core 2 Duo based computer

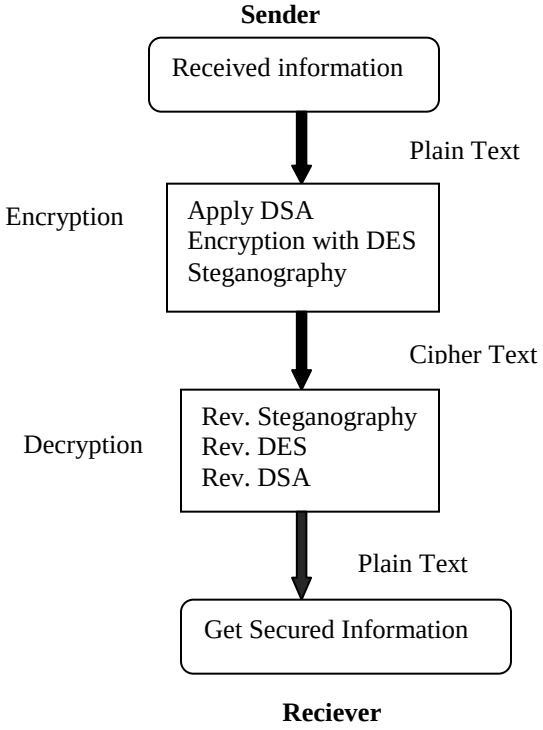

Figure- 3 Proposed Work Design

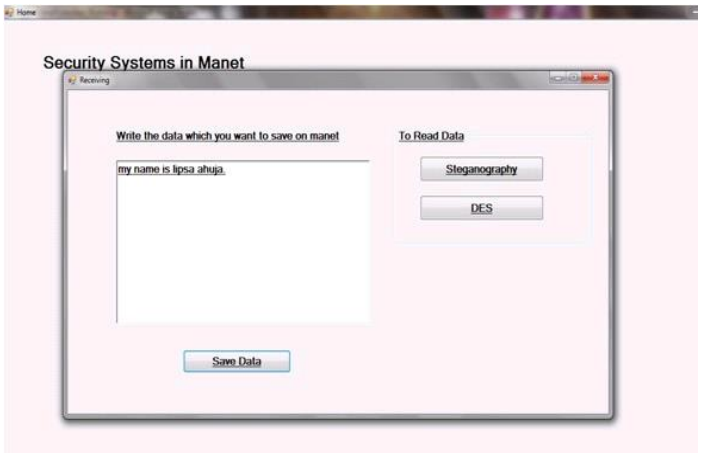

Figure 4- sending routing information

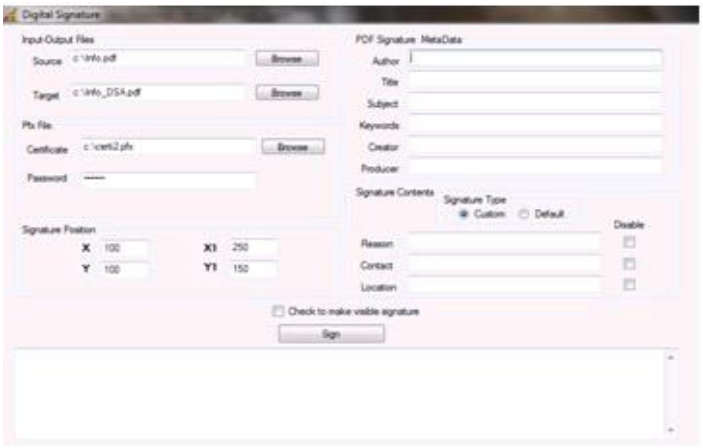

Figure 5- Creating Signed Document

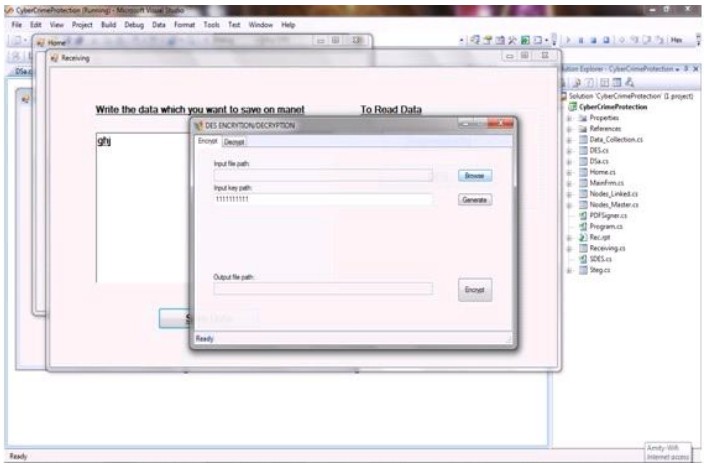

Figure 6- Encryption of signed document

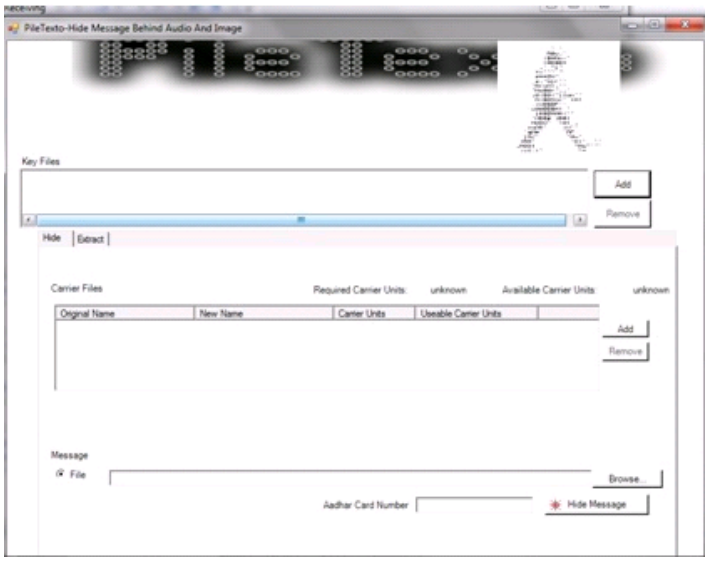

Figure 6- Hiding data behind an audio and image

VI. CONCLUSION AND FUTURE SCOPE

In this paper we implements Digital signature Algorithm, Data Encryption Standard and Steganography to improve the security in cloud computing. 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.

ACKNOWLEDGMENT

We are thankful to our Principal **Dr. S.K Gupta** for providing facilities to wards carrying out this work. We acknowledge the diligent efforts of our head of department **Mr. Dinesh Sorout** in assisting us towards of this idea.

REFERENCES

[1] Amanpreet kaur & Gaurav Raj,"Secure Broker Cloud Computing paradigm Using AES And Selective AES Algorithm" in International Journal of Advanced Research in Computer Science and Software Engineering ISSN:2277 128X, Volume 3, Issue 3, March 2013.

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

[3] 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.

[4] 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.

[5] Neha & Gurpeet Kaur, " Implementing DES Algorithm in Cloud for Data Security", VRSD-IJCSIT, Vol.2(4),2012,316-321.

[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.

[9] Babloo Saha & Shuchi Sharma, "Steganography Techniques of Data Hiding using Digital Images" in Defence Science Journal, Vol. 62, No. 1, January 2012,pp. 11-18.
[10] En.wikipedia.org/wiki/cloud_computing.
[11] en.wikipedia.org
[12] en.wikipedia.orgvocal.com
[13] herongyang.com
[14] acronymfinder.com
[15] abbreviations.com
[16] linktionary.com
[17] courses.cs.tamu.edulinux.about.com
[18] wiki.answers.com

AUTHORS

Khushboo Gupta is a M.Tech student in Computer Science and Engineering at Shri Ram College of Engineering & Management, Palwal.(khushboo9024@gmail.com).
Neha Goyal is a M.Tech student in Computer Science and Engineering at Shri Ram College of Engineering & Management, Palwal.(goyalgirl19@gmail.com)
Puneet Rani is working as an assistant professor in department of computer science in Shri Ram College of Engineering & Management, Palwal,(puneetrani.5270@gmail.com)