Network Coding as a Security Services for Data Security in Cloud

Hetal Patel[1]
[1] Master Engineering of Information Technology
[1] Silver Oak Collage Of Engineering & Technology Ahmedabad Gujarat India

Abstract- *Cloud Computing is trending in today's technology driven world. With the advantages of flexibility, storage, sharing and easy accessibility, Cloud is being used by major players in IT.*

Apart from companies, individuals also use cloud technologies for various daily activities. From using Google drive to store, to Skype to chat and pica web albums, we use cloud computing platforms extensively.

We proposed a design for cloud architecture which ensure secure data transmission for the client organization to the server of the cloud network. We have use combined approach of network coding and steganography because it will be provide a security to the data being transmission on network.

First Data get converted in to coded format through the use of network coding algorithm and coded format data again converted into Stegno images through steganography.

Keywords- Cloud Computing, Security, Network Coding, Stenography

I. INTRODUCTION

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort.

The key concept of cloud computing is that you don't buy the hardware, or even the software, you need anymore, rather you rent some computational power, storage, databases, and any other resource you need by a provider according to a pay-as-you-go model, making your investment smaller and oriented to operations rather than to assets acquisition.

In the cloud computing, there has been huge tread running for the security services, such as a Internet server and cloud-based service in the network, where multiple method are available for securely data transfer in the network. To develop enhanced algorithm for reliability and with steganography module for cloud data storage.

The security concern of the steganography and network coding is major factor for its It Industry Therefore, we use the network coding algorithm to secure data transmission.

The cloud services are shared in one are more customers by pooling in a multitenant environment, which provides virtualized resources to the customer using different technologies. Network coding is one of the most encoding technique for cloud computing. we have work only data security of the reliable Network Coding.

Steganography:

Steganography is the practice of concealinga file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos, meaning “covered, concealed, or protected”, and graphing meaning “wriSteganography:

Steganography is the practice of concealinga file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos, meaning “covered, concealed, or protected”, and graphein meaning “writing”. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganos graphic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganos graphic transmission because of their large size. For example, a sender might start with aninnocuous image file and adjust the colorofevery 100th pixel to correspond to a letter in the alphabet, a change so subtlethat someone not specifically looking for it is unlikely to noticeit.ting”.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

Paper Title:- A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration

Author: Ankit Dhamija, Research Scholar, School of Computer & System Sciences, Jaipur National University, Jaipur

Publisher: IEEE, 2015

Introduction:

In this paper author we propose a design for cloud architecture which ensures secure data transmission from the client organization to the server of the cloud services provider. Author can be used combined approach of cryptography and steganography because it will provide a two way security to the data being transmitted on the network. First, the data gets converted into a coded format through the use of encryption algorithm and then this coded format data is again converted into a rough image through the use of steganography. Moreover, steganography also hides the existence of the message, thereby ensuring that the chances of data being tampered are minimal.

Advantages:

To migrate data on cloud servers through the combined use of cryptography and steganography.
Large security of the data transmission.

Future Work:

In this paper author will put efforts in implementation part of this approach and will try to make comparison of our approach with similar other approaches roposed by fellow researchers.

Paper Title:- Secret Data Sharing in Cloud Environment Using Steganography and Encryption Using GA

Author:- Subhasish MandaI Department of Computer Science & Engineering University Institute of Technology, The University of Burdwan Burdwan, West Bengal, India.
Dr.Souvik Bhattacharyya Department of Computer Science & Engineering University Institute of Technology,The University of Burdwan Burdwan, West Bengal.

Publisher:- IEEE,2015

Introduction:-

In this paper, a crypto-stego methodology has been proposed where image steganography and a new method of cryptographic technique is used. The steganographic technique embedded confidential data using Pixel Mapping Method (PMM), but in a chaotic sequence generated by chaotic map technique. The encryption and decryption uses Genetic Algorithm (GA) which is used to produce a cryptographic method with the help of the powerful features of the Crossover and Mutation operations of GA. Both the encryption and steganography process use secret session key which are generated using the combination of some universal feature of cover image and the users user's secret key.

Future Work:-

In the future work, there is a planning to design a public key data encryption method based on this technique which will targeted to use in highly secure multimedia data transmission applications but that method must have low computational complexity and overcome the database overload headache.

Paper Title :- Secure Cloud Storage Meets with Secure Network Coding

Author:- Fei Chen, Tao Xiang, Yuanyuan Yang, and Sherman S.M. Chow.

Publisher:- IEEE,2016

Introduction:-

This paper reveals an intrinsic relationship between secure cloud storage and secure network coding for the first time. Secure cloud storage was proposed only recently while secure network coding has been studied for more than ten years. Although the two areas are quite different in their nature and are studied independently, we show how to construct a secure cloud storage protocol given any secure network coding protocol. This gives rise to a systematic way to construct secure cloud storage protocols. Our construction is secure under a definition which captures the real world usage of the cloud storage. Furthermore, we propose two specific secure cloud storage protocols based on two recent secure network coding protocols. In particular, we obtain the first publicly verifiable secure cloud storage protocol in the standard model. We also enhance the proposed generic construction to support user anonymity and third-party public auditing, which both have received considerable attention recently. Finally, we prototype the newly proposed protocol and evaluate its performance. Experimental results validate the effectiveness of the protocol.

Future Work:-

In future researches on secure network coding protocols. It is also interesting to study the reverse direction, i.e., under what conditions a secure network coding protocol can be constructed from a secure cloud storage protocol. This possibly requires the latter to have some additional properties.

III. PROPOSED ARCHITECTURE

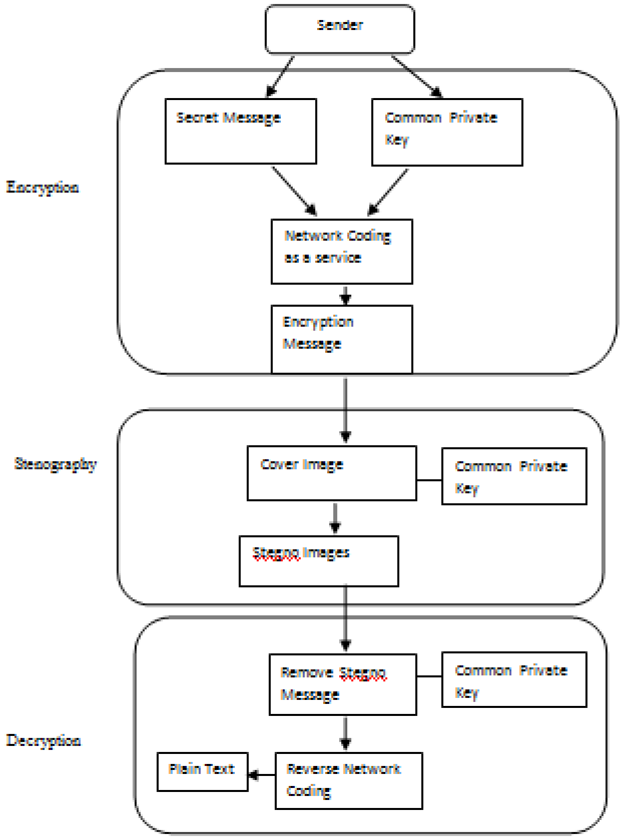


Figure 1. (Proposed Architecture)

Proposed Implementation Methodology Tools & Technologies:

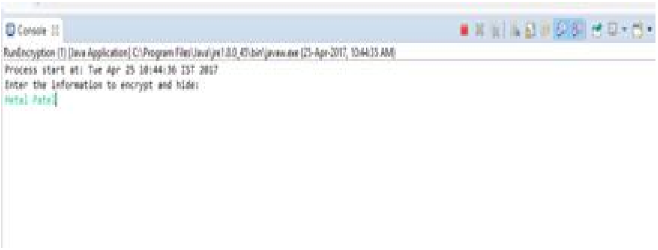
AWS S3
Java
Eclipse

AWS is a toolkit (library) for simulation of Cloud computing scenarios. It provides basic classes for describing data centers, virtual machines, applications, users, computational resources, and policies for management of diverse parts of the system.Allows developers to use JAVA programming language.

System Requirement:

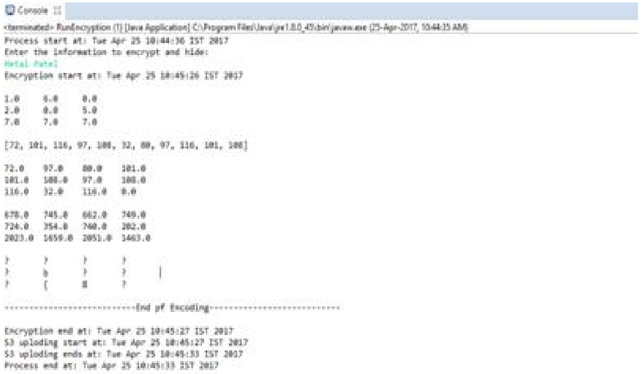
AWS can work on any 32 bit or 64 bit x86 architecture. It can work on any win‘ 10, win‘ 8, win‘ 7, win‘ service pack 2012 having 1 GB of minimum RAM, 1GB of free disk space,. No specific graphics card is required. It has been tested and ran on Sun's Java version 1.8.0 or newer with Eclipse. Older versions of Java are not compatible. If you have non-Sun Java version, such JDK, they may not be compatible. Apache tomcat 8.5.6 is for SQL Server.

IV. IMPLEMENTATION RESULT



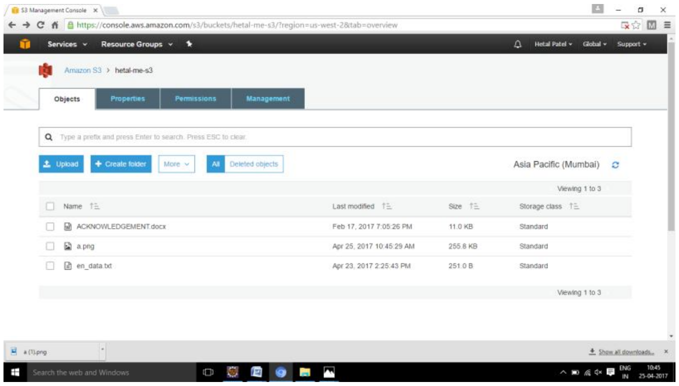
```
Console
RunEncryption (1) [Java Application] C:\Program Files\Java\jre1.8.0_45\bin\javaw.exe (25-Apr-2017, 10:44:35 AM)
Process start at: Tue Apr 25 10:44:36 IST 2017
Enter the information to encrypt and hide:
Hetal Patel
```

Figure 2. (Actual Data File)



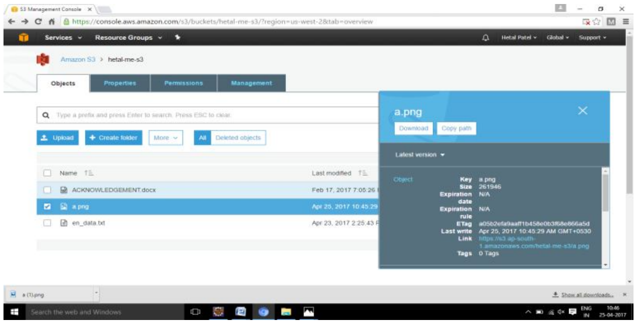
```
Console
<terminated> RunEncryption (1) [Java Application] C:\Program Files\Java\jre1.8.0_45\bin\javaw.exe (25-Apr-2017, 10:44:35 AM)
Process start at: Tue Apr 25 10:44:36 IST 2017
Enter the information to encrypt and hide:
Hetal Patel
Encryption start at: Tue Apr 25 10:45:26 IST 2017

1.0     6.0     0.0
2.0     0.0     5.0
7.0     7.0     7.0

[72, 101, 116, 97, 108, 32, 80, 97, 116, 101, 108]

72.0    97.0    80.0    101.0
101.0   108.0   97.0    108.0
116.0   32.0    116.0   0.0

678.0   745.0   662.0   749.0
724.0   354.0   740.0   202.0
2023.0  1659.0  2051.0  1463.0

?       ?       ?       ?
?       b       ?       ?       |
?       {       8       ?

---------------------------End of Encoding---------------------------

Encryption end at: Tue Apr 25 10:45:27 IST 2017
S3 uploding start at: Tue Apr 25 10:45:27 IST 2017
S3 uploding ends at: Tue Apr 25 10:45:33 IST 2017
Process end at: Tue Apr 25 10:45:33 IST 2017
```

Figure 3. (Encoded File)



Name	Last modified	Size	Storage class
ACKNOWLEDGEMENT.docx	Feb 17, 2017 7:05:26 PM	11.0 KB	Standard
a.png	Apr 25, 2017 10:45:29 AM	255.8 KB	Standard
en_data.txt	Apr 23, 2017 2:25:43 PM	251.0 B	Standard

Figure 4. (Save File In S3 Server)

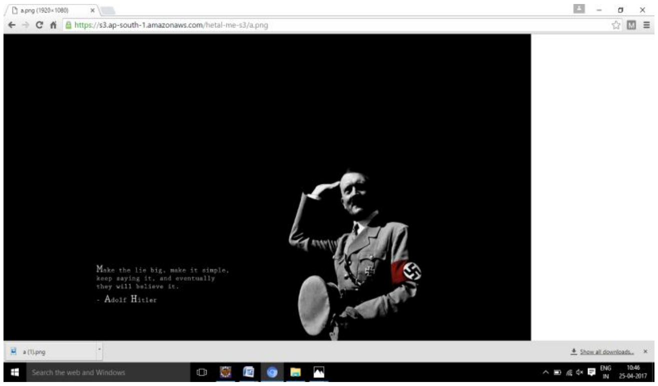


Name	Last modified
ACKNOWLEDGEMENT.docx	Feb 17, 2017 7:05:26
a.png	Apr 25, 2017 10:45:29
en_data.txt	Apr 23, 2017 2:25:43

a.png

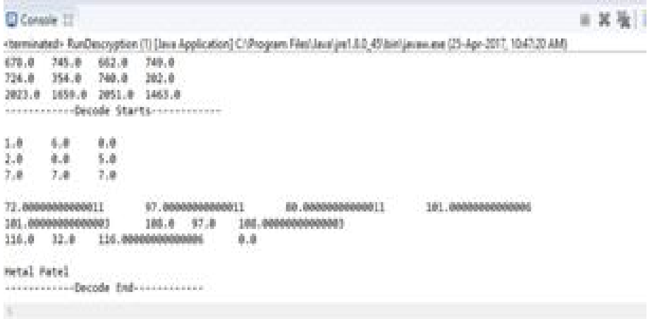
Key	a.png
Size	261946
Expiration date	N/A
Expiration rule	N/A
ETag	a05b2efa9aaff1b458e0b3f68e866a5d
Last write	Apr 25, 2017 10:45:29 AM GMT+0530
Link	https://s3.ap-south-1.amazonaws.com/hetal-me-s3/a.png
Tags	0 Tags

Figure 5. (Start Download File)


a.png (1920×1080)
https://s3.ap-south-1.amazonaws.com/hetal-me-s3/a.png
a (1).png
Show all downloads...
Search the web and Windows

Make the lie big, make it simple, keep saying it, and eventually they will believe it.
- Adolf Hitler

Figure 6. (Encrypted Data File Hide in image)



```
<terminated> RunDecryption (1) [Java Application] C:\Program Files\Java\jre1.8.0_45\bin\javaw.exe (25-Apr-2017, 10:47:20 AM)
670.0   745.0   662.0   749.0
724.0   354.0   740.0   202.0
2023.0  1659.0  2051.0  1463.0
------------Decode Starts------------

1.0     6.0     0.0
2.0     0.0     5.0
7.0     7.0     7.0

72.00000000000011       97.00000000000011       80.00000000000011       101.00000000000006
101.00000000000003      108.0   97.0    108.00000000000003
116.0   32.0    116.00000000000006      0.0

Hetal Patel
------------Decode End------------
```

Figure 7. (Decrypted File)

V. CONCLUSION & FUTURE WORK

In the cloud computing many process available for the data security for the data transmission. In the cloud server using network coding and steganography we can provide more and reliable security in cloud. In the network coding process we can make very simple and effective technique use for data security. We proposed a design for cloud architecture which ensures secure data transmission for the client organization to the server of the cloud network. We have use combined approach of network coding and steganography because it will be provide a security to the data being transmission on network. First Data get converted in to coded format through the use of network coding algorithm and coded format data again converted into Stegno images through steganography.

To implement the working of algorithm on Amazon web service(AWS) and analyze the performance and for network coding. using stegnoghraphy in netwok coding with high security will be extended and data lose will be reduce.

VI. ACKNOWLEDGMENT

I, hereby, take an opportunity to convey my gratitude for the generous assistance and cooperation, that I received from the PG Coordinator Mr. Vikash Tulshyan and to all those who helped me directly and indirectly.

I am sincerely thankful to my Guide, Mr. Darshil Shah for their constant help, stimulating suggestions and encouragement helped me in completing my Literature Review work successfully.

I am also thankful to Mr. Jaimin Dave, Head of the Department and other faculty members who have directly or indirectly helped me whenever it was required by me.

REFERENCES

[1] Abdulzahra H et al, “Combining Cryptography and Steganography for Data Hiding in Images” ACACOS, Applied Computational Science ISBN 978-960-474-368-1

[2] Sherekar et al, Critical Review of Perceptual Models for Data Authentication,Emerging Trends in Engineeringand Technology (ICETET)2nd International Conference, 2009, pp. 323-329. IEEE.

[3] Usha, S., Kumar, G. A. S., and Boopathybagan, K., A secure triple level encryption method using cryptography and steganography, Computer Science and Network Technology(ICCSNT), International Conference, Vol.2, No.2.11, 2011 ,pp. 1017-1020.IEEE.

[4] Bharti,P.,andSoni, R.,A New Approach of Data Hiding in Images using Cryptography and Steganography,InternationalJournalofComputer Applications, Vol.58,No.18,2012,pp1-5

[5] Marwaha, P., Visual cryptographic steganography in images,Computing,Communication and Networking Technologies(ICCCNT), International Conference , 2010,pp 1-6. IEEE.

[6] Umamaheswari, M., Sivasubramanian, S. and S. Pandiarajan S., Analysis of Different Steganographic Algorithms for Secured Data Hiding,IJCSNS International Journal ofComputer Science and Network

Security, Vol.10, No.8, 2010, pp 154-160.

[7] Domenico Daniele Bloisi, Luca Iocchi, "Image based Steganography and cryptography", Computer Vision theory and applications volume I, pp. 127-134 .

[8] Souvik Bhattacharyya, Lalan Kumar and Gautam Sanyal, "A novel approach of data hiding using pixel mapping method (PMM)"

[9] http://www.rfwireless-world.com/Tutorials/public-cloud-vs-private-cloud-vs-hybrid-cloud-vs-community-cloud.html

[10] Spillman R,Janssen M, Nelson B and Kepner N, "Use of Genetic Algorithm in Cryptanalysis of Simple Substituion Cipher" Cryptologia, Vol.l7, No.4, pp. 367- 377, 1993.

[11] Spillman R,"Cryptanalysis of Knapsack Ciphers using Genetic Algorithms", Cryptologia, VoU7, No.4, pp. 367-377, 1993.

[12] Y. News. (2013). Cloud computing users are losing data, symantec finds [Online]. Available: http://finance.yahoo.com/news/ cloud-computing-users-losing-data-205500612.html

[13] [13] P. Hernande. (2013). Byod, data loss top list of cloud computing challenges [Online]. Available: http://www.datamation.com/ cloud-computing/byod-data-loss-top-list-of-cloud-computingchallenges.html

[14] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacypreserving public auditing for secure cloud storage,” IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[15] N. Cai and R. W. Yeung, “Secure network coding,” in Proc. IEEE Int. Symp. Inf. Theory, 2002, p. 323.

[16] C. Gkantsidis and P. R. Rodriguez, “Cooperative security for network coding file distribution,” in Proc. IEEE Int. Conf. Comput. Commun., 2006, pp. 1–13.