International Journal of Pure and Applied Mathematics
Volume 119 No. 14 2018, 1653-1660
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

SECURE DATA TRANSMISSION BY STEGANOGRAPHY USING PRIVATE KEY IN CLOUD

Balaji. S[1], Mandy Sonio Newcastle[2]
Research Scholar[1],Assistant Prof[2], Dept of Information Technology, Biher University

ABSTRACT

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements.Cloud computing security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations. To overcome this security issue, Cryptography and Steganography with private key is used to securely transfer data over malicious environment. This technique can yield 95% security to enhance security in data transmission.

INTRODUCTION

Cloud computing [7-14] is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. Cloud computing security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations.

The existing system presents a generic data lineage framework for data flow across multiple entities that take two characteristic, principal roles (i.e., owner and consumer) [2]. The exact security guarantees required by such a data lineage mechanism toward identification of a guilty entity, and identify the simplifying non-repudiation and honesty assumptions[3]. They develop and analyze a novel accountable data transfer protocol between two entities within a malicious environment by building upon those principal roles. The identification of the leaker is made possible by forensic techniques [4], but these are usually expensive and do not always generate the desired results. Therefore, we point out the need for a general accountability mechanism in data transfers.

The main idea is to transfer the data in secured manner over a malicious environment in cloud using steganography and cryptography. The data to be sent is encrypted and steganography is applied over the data. The private key generated is sent to the authorized receiver who requests the auditor. The original data can be retrieved only after applying the private key over the encrypted data.

A. RELATED WORK

Chen Shuai and Zhong Xian-xin [1] proposed the order to enhance safety and improve the multimedia wireless sensor information confidential and information processing speed, the research of wireless sensor data encryption chip core. Under the action of key, the chip can encrypt plaintext and decrypt cipher text from the input port properly. First of all, this paper analyzes the encrypted multimedia sensor chip architecture. Secondly introduces the design principle of the chip, and analyzes the key randomness.

Chippy Jacob and Rekha V. R [2] proposed Data de-duplication technique has been used widely which allows only storing a single copy of a file and thus avoids duplication of file in the cloud storage servers. It helps to reduce the amount of storage space and save bandwidth of cloud service and thus in high cost savings for the cloud service subscribers. So data encryption by data owners with their own keys makes the de-duplication impossible for the cloud service subscriber as the data encryption with a key convert's data into an unidentifiable format called cipher text thus encrypting, even the same data, and with different keys may result in different cipher texts.

Nandita Sengupta and Jeffrey Holmes [3] proposed as number of users is increasing for cloud computing, threat

for protecting confidential data in cloud is also increasing. This has led the computer scientists and researchers to think for finding robust security system for cloud computing. This cryptographic security system is designed in such a way so that computation time for decryption of ci`pher text messages for the hackers will be more compared to any single cryptographic system.

Akshita Bhandari et al. [4] proposed Cloud computing is a rising technology that is still unclear to many security issues. The most challenging issue today in cloud servers is to ensure data security and privacy of the users. The goal of this paper is to use various cryptography concepts during communication along with its application in cloud computing and to enhance the security of ciphertext or encrypted data [15-19] in cloud servers along with minimizing the consumption of time, cost and memory size during encryption and decryption.

Zhihua Xia et al. [5] proposed the increasing importance of images in people's daily life, Content-based Image Retrieval (CBIR) has been widely studied. Compared with text documents, images consume much more storage space. Hence, its maintenance is considered to be a typical example for cloud storage outsourcing. For privacy-preserving purposes, sensitive images, such as medical and personal images, need to be encrypted before outsourcing, which makes the CBIR technologies in plaintext domain to be unusable. In this paper, we propose a scheme that supports CBIR over encrypted images without leaking the sensitive information to the cloud server.

B. PROPOSED SYSTEM

Identification of the leaker is made possible by forensic techniques, but these are usually expensive and don't always generate the desired results. Therefore, we point out the need for a general accountability mechanism in data transfers. This accountability can be directly associated with provably detecting a transmission history of data across multiple entities starting from its origin. This is known as data lineage or source tracing.

This system consists of following three

a) Sender
b) Auditor
c) Receiver

The sender sends the text message along with the image to the authorized receiver. The text sent is encrypted and hidden within the image. When the user registers a new login, by default the user is blocked. To remove the block the auditor checks if the user is authorized or not. Auditor allows only the authorized user to send and receive the messages. Image received by the end user will contain the encrypted text which can be retrieved only when requests key to the auditor. The auditor verifies the request sent by the receiver and sends the private key to the requester only if he is authorized. The authorized receiver submits the key to reveal the encrypted text hidden in the image. Some random text will be generated in the message box so that the direct sent text will be hidden somewhere in the message box. To retrieve the message, we have to decrypt the text with the private key in display box.A novel accountable data transfer protocol between two entities within a malicious environment is build to enhance oblivious transfer, robust watermarking, and signature primitives. This method helps to securely transfer data without any leakage.

C. ARCHITECTURE

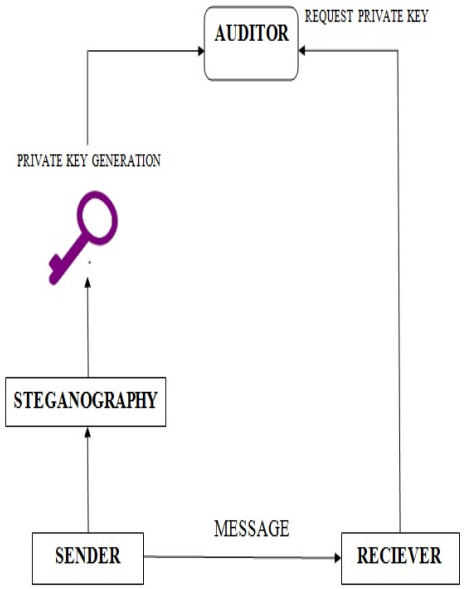


Fig 1 ARCHITECTURE

This system as shown in Fig 1 supports data transfer in malicious environment by Cryptography and Steganography using private key. The sender sends the

message to the user which is managed by the intermediate auditor who verifies that the receiver is authorized and sends the key to access the data.

D. ALGORITHM

There are two main algorithms used in this system for Cryptography and Steganography. They are as follows:

IMAGE DOMAIN ALGORITHM

1st step: Convert the data from decimal to binary. [Message] [1000001]

2nd step: Read Cover Image

3rd step: Convert the Cover Image from decimal to binary.

10010000 10011010 10011100 10010010 10010110
10011101 10101111 10100101 10100000 10011011
10011111 10100010 10000101 01111011 10000101
10010001 10010000 10001101 10001101 10001010
00111101 00110111 01000001 01001111 01111000
01111011 10000011 10010000 00110010 00111101
01001010 01011100 10101010 10100111 10100111
10100110 00111101 00111011 00111000 00111011
01111000 01111101 10000011 10000100 00111101
00111011 00111011 00111011 01111100 10000101
10000111 10000011 01011000 01001100 01001101
01001100 10001010 10011001 10100111 10011010
10001011 ……..... ……..... …….....

4th step: Break the byte to be hidden into bits. Thus [10000001] [1 0 0 0 0 0 0 1].

5th step: Take first 8 byte of original data from the Cover Image.

10010000 10011010 10011100 10010010 10010110
10011101 10101111 10100101

6th step: Replace the least significant bit by one bit of the data to be hidden.

- First byte of original data from the Cover Image:
- First bit of the data to be hidden:
- Replace the least significant bit:
- Repeat the replace for all bytes of Cover Image:
- Finally the cover image before and after steganography.

This is divided into 8 bits 1 0 0 1 0 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 1 0 0 1 1

EMBEDDING ALGORITHM

Step 1: Extract Bit set of Message, Bit = {M0, M1… M65535}

Step 2: The Pixels of cover image, Pixel = {pixel0, pixel1… pixel65535}

Step 3: Extract LSB-1 set of the cover image, LSB1 = {A0, A1… A65535}.

Step 4: Extract LSB-2 set of the cover image, LSB2 = {B0, B1… B65535}.

Step 5: For i=1 to message length
do
{
If Mi= =Bi
Then do nothing
Else
{
If Mi= =1 and Bi= =0
Then
{
Bi=Mi; Ai=0; Pixel (i) =1
}
Else If Mi= =0 and Bi= =1
Then
{Bi=Mi; Ai=1; Pixel (i) +=1}
}
}

E. IMPLEMENTATION AND RESULTS

The proposed system is implemented with these algorithms to transfer data securely over malicious environment. The data to be sent is hidden within an image in an encrypted form. The private random key is generated for every steganographed image.

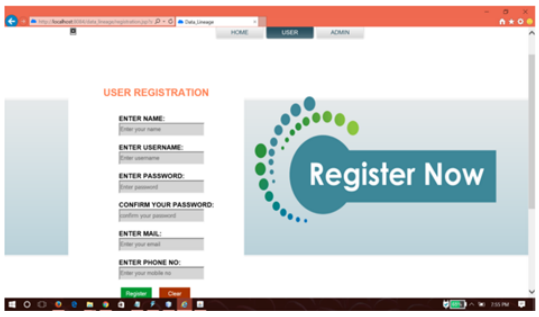
The receiver requests the key from the auditor. When the auditor verifies that the receiver is authorized he sends the key. The data can be revealed and decrypted by the key using the tool.

The proposed system has been successfully implemented to transfer the data securely over malicious environment.

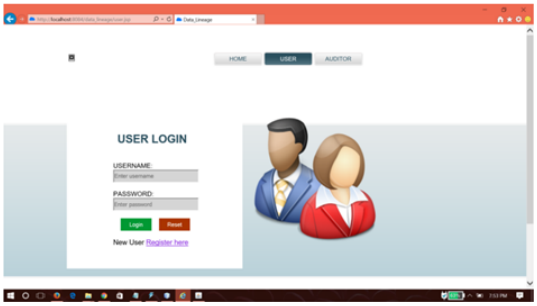
F. SCREENSHOTS

I. Sender Module

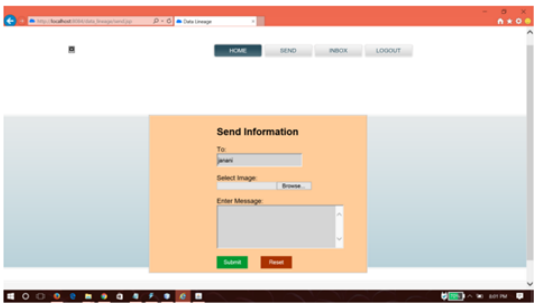
a) Registration



b) User Login

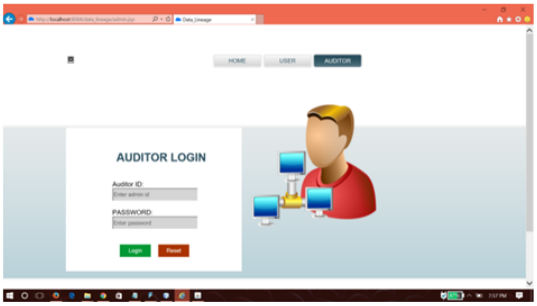


c) Sending The Information

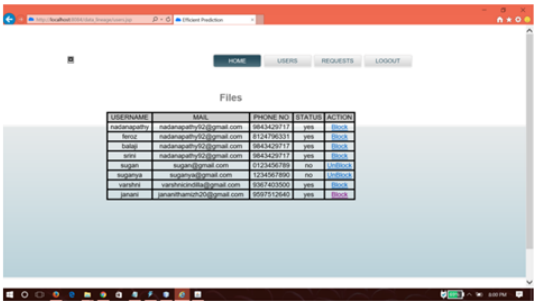


Auditor Approval Module

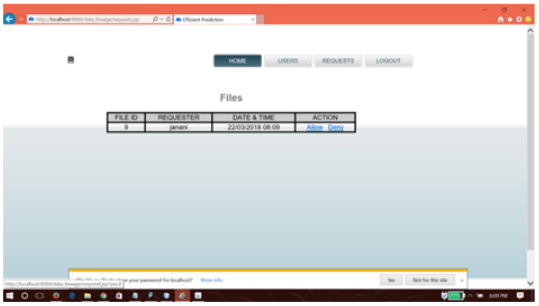
a) Auditor Login



b) User Registration Approval

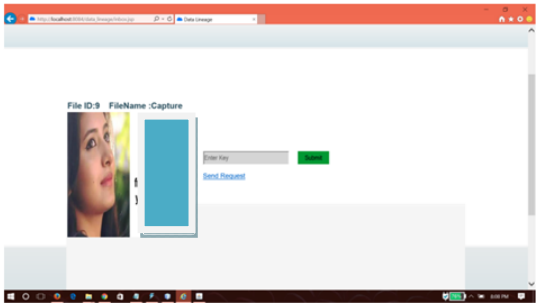


c) Key Request

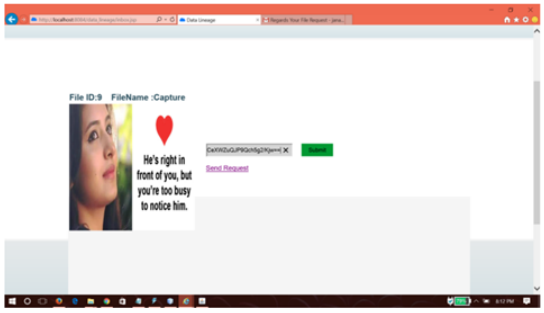


II. Receiver Module

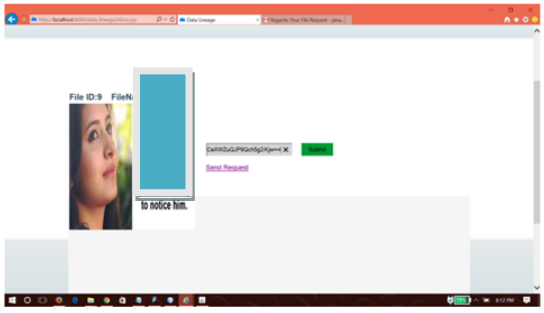
a) Receiver Inbox



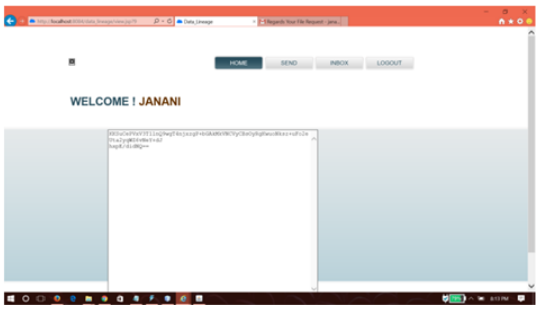
b) Key Mailed To Authorized Receiver



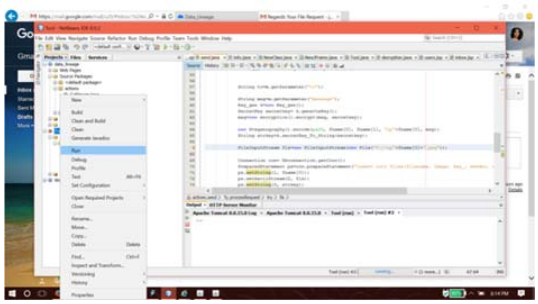
c) Key Submittion



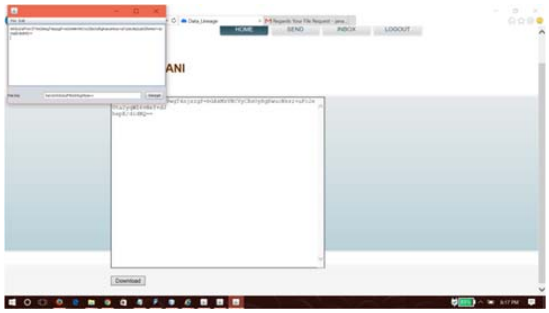
d) Encrypted Text



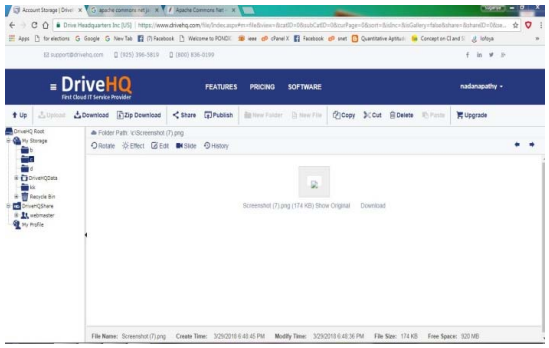
e) Tool To Decrypt Th Encrypted Text



G. Original Text Revealed In Display Box



H. Cloud Storage



G. PERFORMANCE ANALYSIS

1. The Steganography technique is used to increase the reliability and reduce the noise in the transmission.
2. The Cryptography is used to encrypt and decrypt the message to maintain the security of confidential data.
3. In this proposed system, Cryptography and Steganography are applied to ensure higher level of security.

4. The private key used for Steganography prevents the chances of illegal access.
5. The auditor sends the key only after verifying that the receiver is authorized, so it halts the illicit users.

H. EXISTING GRAPH

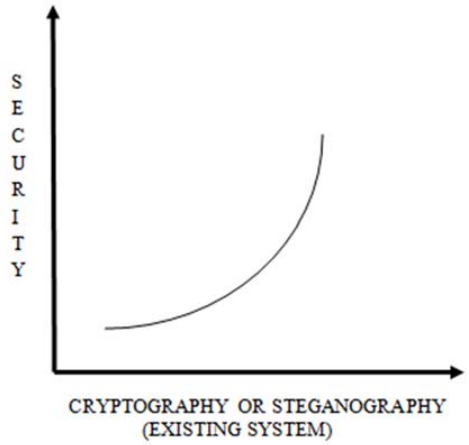


FIG 2 EXSTING SYSTEM GRAPH

The existing system makes use of either Steganography or Cryptography for security as shown in FIG 2. They provide only less amount of security for transferring data over malicious environment.

I. PROPOSED SYSTEM GRAPH

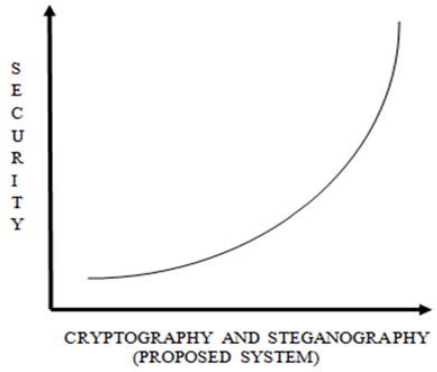


FIG 3 PROPOSED SYSTEM GRAPH

The proposed system makes use of both Steganography and Cryptography for security. The Steganography used generates private key to reveal the data. Hence, the security is increased in this system as shown in FIG 3.

J. CONCLUSION

The proposed system acts as a sound technique to transfer the data over malicious environment. A private key is generated for each Steganographed image which can be obtained from the auditor by only authorized users. The advantage of the system is that it provides increased security. The future work is to support all the formats of data transfer over hostile domain.

REFERENCES

[1] CHEN Shuai, “Research of Cipher Chip Core for Sensor Data Encryption” DOI 10.1109/JSEN.2016.2539391, IEEE Sensors Journal.

[2] Chippy Jacob , Rekha V. R “ Secured and reliable file sharing system with deduplication using erasure correction code”, 2017 International Conference on Networks & Advances in Computational Technologies , Trivandrum.

[3] Nandita Sengupta, Jeffrey Holmes “Designing of Cryptography Based Security System for Cloud Computing” 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies.

[4] Akshita Bhandari, Ashutosh Gupta, Debasis Das “Secure Algorithm for Cloud Computing and Its Applications “ , 2016 IEEE.

[5] Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin “A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing” , IEEE transcation on information forensic and security, september.

[6] L. Ji, S. Kolhe, and A. D. Clark, “Data Analysis of Cyber-Activity within High Performance Computing Environments” 2017 IEEE.

[7] Vigneshwaran, R., Janakiram, A., Jarina, S., Prem Kumar, K., Anantharaj, B., Sathian, D., "An empirical analysis on Quality of Service(QoS) in cloud computing", (2016) Indian Journal of Science and Technology, 9 (22), art. no. 95181,

[8] Karthikeyan, P., Sathian, D., Raghav, R.S., Abraham, A., Dhavachelvan, P., "A comprehensive survey on variants and its extensions of BIG

DATA in cloud environment", (2015) ACM International Conference Proceeding Series, 06-07-March-2015, art. no. 2743097,

[9] Padmapriya, V., Bakkiya, K., Sujitha, B., Thamizhselvi, M., Premkumar, K., "A scalable service oriented consistency model for cloud environment (SSOCM)", (2015) ACM International Conference Proceeding Series, 06-07-March-2015, art. no. 2743089,

[10] Ilamathi, R., Moganarangan, N., Ravishankar, V., Baskaran, R., Premkumar, K., "Performance analysis in cloud auditing: An analysis of the state-of-the-art", (2015) International Journal of Applied Engineering Research, 10 (3), pp. 2043-2046.

[11] Kathavate, P., Reddy, L.S.S., Satyanarayana, K.V.V., "Effects, challenges, opportunities and analysis on security based cloud resource virtualization", (2017) Journal of Advanced Research in Dynamical and Control Systems, 9 (Special Issue 12), pp. 1458-1463.

[12] Garikapati, G., Yakobu, D., Nitta, G.R., "An analysis of cloud data security issues and mechanisms", (2017) International Journal of Pure and Applied Mathematics, 116 (6 Special Issue), pp. 141-147.

[13] Ramya, U., Reddy, B.T., Sekhara Rao, M.V.P.C., "Enhanced check sum approach for secure deduplication file system in integrated cloud system", (2017) Journal of Advanced Research in Dynamical and Control Systems, 9 (Special Issue 6), pp. 322-334.

[14] Sandhya, A., Harshini, T., Vyshnavi, T., Vurukonda, N., Rao, B.T., "Scalable attribute based encryption scheme for accessing cloud data", (2017) International Journal of Pure and Applied Mathematics, 115 (8 Special Issue), pp. 541-546.

[15] Padmapriya, V., Gowri, V., Lakshmipriya, K., PremKumar, K., Thiyagarajan, B., "Perspectives, motivations and implications of big data analytics", (2015) ACM International Conference Proceeding Series, 06-07-March-2015, art. no. 2743099,

[16] Rao, D.N., Sathian, D., Dhavachelvan, P., Raghav, R.S., Prem Kumar, K., "Big data scalability, methods and its implications: A survey of current practice", (2015) ACM International Conference Proceeding Series, 06-07-March-2015, art. no. 2743121,

[17] Karthikeyan, P., Sathian, D., Raghav, R.S., Abraham, A., Dhavachelvan, P., "A comprehensive survey on variants and its extensions of BIG DATA in cloud environment", (2015) ACM International Conference Proceeding Series, 06-07-March-2015, art. no. 2743097,

[18] Padmapriya, V., Gowri, V., Lakshmipriya, K., Vinothini, S., PremKumar, K., "Demystifying challenges, opportunities and issues of Big data frameworks", (2015) ACM International Conference Proceeding Series, 06-07-March-2015, art. no. 2743110,

[19] Bandi, R., Gouse, S., "A comparative analysis for big data challenges and big data issues using information security encryption techniques1, 2", (2017) International Journal of Pure and Applied Mathematics, 115 (8 Special Issue), pp. 245-251.