ISSN 2395-1621

Network Security Using Scanning Pattern and Matrix Mapping Method

[#1]Aditya Anthony, [#2]Shubham Choudhary, [#3]Nikhil Gandhi, [#4]Rahul Kolte

[1]aditya.anthony7@gmail.com
[2]shubhamchoudhary13695@gmail.com
[3]nikhil.gadhi157@india.com
[4]kolterahul1995@gmail.com

[#1234]Student, Department of Computer Engineering

GHRCEM, Wagholi, Pune

ABSTRACT

Now-a-days data security is very important and high prioritized topic. Multimedia security is an important field of research in the area of information sharing. As computer technologies of new world require communication for making them work efficiently. There is a humongous data transaction over Internet, Teleconferencing, TV, Smartphones, pervasive devices, military and telemedicine applications. To prevent the confidentiality, integrity and authenticity of data from getting exploited, Encryption is one of the uninterrupted and straightforward way to give the security to data; keeping this consciousness in mind we volunteer with a hybrid avenue for data encryption. This paper presents a survey of over various research papers dealing with data and image encryption techniques in which each technique has its own merits and demerits. It additionally focuses on the functionality of data decryption and encryption technique.

ARTICLE INFO

Article History

Received: 10th May 2016

Received in revised form :

10th May 2016

Accepted: 13th May 2016

Published online :

14th May 2016

Keywords: **Mapping, Scan Patterns, Multimedia Security, Encrypt data, Decrypt data.**

I. INTRODUCTION

Using a Network huge data, such as text or multimedia data is shared every day among computers. As the transmission ability of a network increases the information is made available lucidly to every users on demand. The amount of multimedia data sharing is increasing day by day. Most of the commercial transaction is carried out online, studies in 2016 showed that 67% of overall transactions were made online and of which 27% were made using smartphones. As a result there is a need for higher quality of security in this field. Using encryption users can ensure that no unauthorized user can sniff or spoof their data in transmission over the network i.e it provides a reliable and secure way for transmission of data. The unauthorized attacks has increased over these few years, which has given a rise to demand of new, powerful, complex and secure encryption techniques.

II. PROPOSED SYSTEM

It is Client-Server Based Model. In which Server is responsible for servicing the requests form the client side and performing following tasks:

- Authentication.
- Encryption.
- Decryption.

Users can access server from any device (eg: cell phone, laptop, etc.).

There are two categories of users:

Registered Users:

These users have the authority to perform encryption and decryption.

Guest Users:

These users use OTP (one time password) to decrypt the file which is shared by the registered user. These users can only decrypt file.

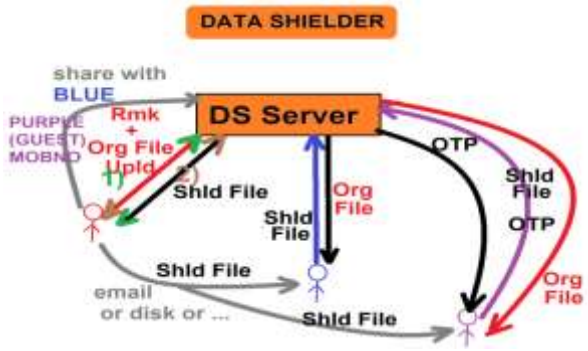

Fig 1. Architecture or Overview

III. ALGORITHM

Once a user is registered and wants to encrypt a file, he/she needs to add a remark and select any type of file that he/she wants to protect and upload it on the server. After uploading the encryption process will start; this encryption process includes generation of a key, which will the use for unique identification of the file, key is generated by using the remark provided by the client and the client image, and once the process is done the protected file will be returned.

If the same user wants to decrypt the fine in near future he needs to select the remark that he/she gave during the encryption process and upload the encrypted file. After uploading the server will apply the decryption process on the encrypted file and return the original file.

Now let's go in detail of the encryption-decryption process.

Encryption

1) Using the key we'll generate a mapping matrix. Every byte of the mapping data is unique and is taken with respect to key. The mapping matrix is of size 16 by 16.

2) The source file is opened for reading in binary mode.

3) Every byte of the source file is read and converted into its equivalent 8-bit binary number.

4) Split the 8-bit binary number into 4-bit higher and lower nibble number.

5) Convert these two 4-bit nibbles into its equivalent decimal value.

6) With the help of these 2 decimal values pick-up a pixel from the mapping matrix. Where the decimal equivalent higher nibble acts as the row indicator and the decimal equivalent lower nibble acts as column indicator for mapping data bytes.

7) Replace the original byte with the byte selected from mapping matrix.

8) Encrypted file gets generated as the above process is repeated for all the pixels.

Following are the step by step snap shots of working of this system:

GUI screens of the Web application:

Fig 2. Login page

Fig 3. Welcome page

Fig 4.Shielding step-1

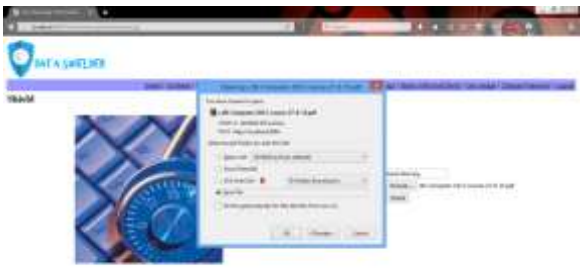

Fig 5. Shielding step-2

Fig 6. Un-shielding step-1

Fig 7. Unshielding step-2

Fig 8. Un-shielding step-3

Fig 9. Sharing with Client step-1

Fig 10. Sharing with client step-2

Fig 11. Un-shielding after sharing step-1

Fig 12. Un-shielding after sharing step-2

Fig.13. Un-shielding after sharing step-3

Fig 14. Un-shielding after sharing step-4

Fig 15. Sharing with non-client step-1

Fig 16. Sharing with non-client step-2

Fig 17. Logout

Decryption

1) Using the key we'll generate a mapping matrix. Every byte of the mapping data is unique and is with respect to key. The size of mapping matrix is 16 by 16.
2) The encrypted file is opened for reading in binary mode.
3) Every byte of the encrypted file is taken into consideration individually and converted into its equivalent 8-bit binary number.
4) Match the byte in the mapping matrix and find out row and column number of the matched byte.
5) Form 2 nibbles using the row and column number, Generate a 8-bit binary number from 4-bit higher (row) and lower (col) nibble number.
6) Substitute this generated 8 bit binary data in place of the current byte.
7) Original file gets generated by repeating the process for all the pixels.

IV. ACKNOWLEDGEMENT

We have taken efforts in this project. However, it would not have been possible without the kind support and help of Prof. Ganesh Bandal. We would like to extend my sincere thanks to him."We would like to thank Professor Urmila Biradar for her expert advice, encouragement and support throughout this difficult project."

V. CONCLUSION

The security for the digital data has become highly important since the communication by transmitting of digital products over the open network occur very frequently. To avoid reading, alteration of data, adding false information or deleting part of data, encryption is needed. So it is necessary to develop new and evolving encryption technique which are fast and secure with high rate of security.

REFERENCES

[1]Jing-Jang Hwang, Taoyuan, Taiwan,Yi-Chang Hsu, Chien-Hsing Wu, ABusiness Model for Cloud Computing Based on a Separate Encryptionand-Decryption Service, in International Conference on InformationScience and Applications (ICISA), pages 1-7, 2011.

[2] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems ", The Journal of Systems and Software 58 , 83-91,2001.

[3] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations", IEEE Proceeding in the year 2003.

[4] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27, 2007.

[5] P. Zimmerman, "An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999.

