CLOUD SECURITY USING LEAST SIGNIFICANT BIT STEGANOGRAPHY AND DATA ENCRYPTION STANDARD ALGORITHM

Hambali Moshood Abiola[1],*, Gbolagade Morufat Damola[2], Olasupo Yinusa Ademola[3]
[1, 3,] Computer Science Department, Federal University Wukari, P.M.B 1020, Katsina-Ala Road, Wukari, Taraba State, Nigeria
[2.] Department of Computer Science, Al-Hikmah University, P.M.B 1601, Adewole Housing Estate, Ilorin, Kwara State, Nigeria.
E-mail addresses: [1]hambali@fuwukari.edu.ng [2]dammyconsult@gmail.com, [3]yinusa@fuwukari.edu.ng
*Corresponding Author

ABSTRACT

Cloud security is getting more important than ever before. The cloud platform and services are regards as massive accessible data centers that can be accessed anywhere and anytime. The increase in the cloud users has unfortunately also, been accompanied by the growth in malicious activities in the cloud. Millions of people are surfing the cloud for different purposes, hence they need a highly secured environment and consistent services. The future trend of cloud computing, especially in expanding the series of applications that requires a deeper degree of privacy and authentication. Cryptography and steganography are the two famous security measures to prevent unauthorized users to access information in the cloud. The goal of cryptography is data protection while that of steganography is to enable secret communication. Cryptography transforms the original data into an unreadable format (that is, ciphertext) to the typical user whereas steganography embedded a vital message in other digital media. We proposed a simple data protection model where data is encrypted using data encryption standard (DES) and least significant bit (LSB) steganography. The proposed model was able to provide two layer security strength to the documents by preventing unauthorized users from gaining access to the documents in the cloud.

Keyword: *DES*, *LSB*, AES, Encryption Standard-Mobile Phone keypad (AES – MPK).

1. INTRODUCTION

One of the evolving technologies today is cloud computing which is a technology subset of information technology. Cloud computing can be described as abstraction of computer and internet network that masked complex infrastructure (Basri, Mawengkang & Zamzami, 2018), that allows one to store, update and share information or build applications within a virtual server, managed by a cloud computing service provider. Cloud computing is basically rendered access to resources like server, networks, operating system, software applications and efficient storage space used by the user's payable on demands (Nancy & Kamalinder, 2016) and can be accessed anywhere, anytime and with any device, all it requires is only browser applications (Mathew, 2012).

Security in the cloud computing environment is a very vital and crucial aspect due to the significance of data stowed on the cloud and this data may be confidential and extremely sensitive. Therefore, there is a need for completely reliable data management and security protection for the data in the cloud. Though, there are some threats such as data theft known as breach/loss data may occur (Kaur & Singh, 2015). In this regard, the users are seriously concern, as they don't know who is accessing their data and whether changes are made on the data since the third party has full control on the data once it is sent to the cloud (Arockiam & Monikandan, 2013). There are two

major threats attack in which the security of data in the cloud can be of concern. The first one is internal and the second is the external threat. The most common attack is the internal attack caused by the cloud service provider administrator who may illegally have access to the user's data in the cloud. The second is caused by hackers. The hackers are the external intruders who might gain illegal access to the resources in the cloud (Vinita, Ali & Sharma, 2016). Omer, Safia, El-Sayed & Abdel-Badeh (2013) stated that to ensure the securities of data in the cloud, the three important parameters involved are: confidentiality, integrity and availability. In confidentiality, this is to make sure that data is only accessible by the intended user. Integrity ensures that the content of the data is unchanged when accessed by the user. In the case of availability, it ensures that data is always ready anytime, anywhere on the cloud. Adamu & Boukari (2017) opined that there is need to address the security challenges which is in form of malicious activities, vulnerabilities and increasing security advisories coupled with the lack of confidentiality, integrity and availability of data downloaded and uploaded into the cloud has become necessary to ensure highly safe and persistent service.

Both Cryptography and Steganography has been the major means of protecting data. Though, they are considered to be of different techniques of securing data because they have a distinct goal which makes them different. Cryptography systems convert original data into Ciphertext. So that only genuine users with the correct key can gain access to data from the cloud server storage. The main aim of cryptography is to hinder hackers, online/software crackers, and any third party users from accessing the data by changing the data to an unreadable format. Nevertheless, cryptographic encryption methods can also be attacked using brutal force or cryptanalysis attacks that predict the algorithm employed for message encryption or try to break the key used for encryption. To reinforce the cryptography technique, it is necessary for an additional layer of security which is the steganography techniques. Steganography is concerned with concealing the existence of secret information within computer files through other media (Ravi & Murti, 2011) to successfully transfer data to the cloud without drawing the attention of intruders. To get access to the concealed data, the user has to verify the data with the private key, on successful validation, the Steganography file will be extracted and decryption of the content of the data will be done using the private key. Then user data will be secure in the cloud using DES algorithm as a digital signature. Therefore, this study employs DES and LSB to form a combine cryptography and steganography technique to improve the security of data in the cloud.

2. RELATED WORK

There are lots of approaches and methods that have been used to implement encryption or steganography using various digital communication contents.

Satwinder & Varinder (2015) proposed a dual-layer approach to security of data. The Least Significant Bit (LSB) image steganography was used for the first layer to encode the data. In the second layer, the Advanced Encryption Standard (AES) algorithm was proposed and this provides the encryption of data. Steganography was only used as additional security to the communication channel but not for the encryption of data, a secret text message was hidden behind digital image file and it was later encrypted using an advance encryption standard algorithm.

Marwa, Abdelmgeid & Fatma (2016) proposed improved steganography and cryptography. They introduced a modified advanced encryption standard (AES) algorithm. The secret message is encrypted with the introduction of Advance Encryption Standard _Mobile Phone keypad (AES – MPK) after which the encrypted message is hiding behind a grey image using Pixel Value Difference (PVD), MPK and MSLDIPMPK.

To prevent the prevalent from hacker entry into a communication channel, a combination of steganography and cryptographic was used as a measure to secure data (Sasikumar & Vijayanandh, 2017). This combined method provides a sophisticated approach for secret message interchange within transmitter and receiver. In this approach, nested image steganography was introduced which is carried out by placing a Quick Response (QR) message on a cover image. The

established method has a great peak signal to Noise Ratio (PSNR), mean square error (RMSE) subsist chi-square quantity with 100% recovery of the message.

Aiswarya & Hema (2017) analysed and proposed the power of conjoining the two popular methods of securing data from intruders. It was stated that while steganography provides secret communication, cryptography is used to establish protection to the data by converting the data into ciphertext.

A robust and secure method was initiated to hide secret information in digital multimedia content (Ahmed & Talal, 2017). The advantage of combining cryptography and steganography was utilized in this scenario. Firstly, the secret text message was encrypted using AES (Advanced Encryption Standard) algorithm and SHA-2 was used to hash the key from attack. They later provide an additional key to make the hiding process non-sequential.

Babatunde, Taiwo & Dada (2018) presented a combination of 3DES and LSB to improve security measure on medicinal data. A simulation program was developed during the experiment using the Java programming language. The result of the experiment showed that using a combined model, the medicinal records can be managed and properly secured.

Improved steganography using the least significant bit is implemented by Ngatia & Njuguna (2018). They evaluate the integrated randomization algorithm to develop the LSB technique. The algorithm used the binary codes representing the pixel in the image. The stego image in the form of binary representation is covered within another image, that is, the cover image. The bit of the secret image was made to disperse and prevent the access of unauthorized users. The hiding image is regenerated and the quality of the data is finally conserved.

Basri, Mawengkang & Zamzami (2018) proposed and demonstrated the combined method of DES and LSB for the confidentiality and security of data on the cloud. They stated that the limitation of storage source account for storing data in the cloud, thus securing data in the cloud is highly necessary to prevent the brute force attack. The DES is used as a standard symmetric encryption algorithm. It utilizes the 16 rounds algorithm which is prone to a brute force attack. The 16 round algorithms will not be processed until it is converted to ciphertext. LSB algorithm is then used to hide image under the smallest bit of the cover image. The combination of these two methods helps to protect and secure data on the cloud.

Ahmed (2018) work on the combination of both steganography and cryptography using the dual as a mean of providing security to the data transmission system. The high profile methodology used was the bitmap (BMP) steganography and substitution encryption. The approach was that the text message and the so-called mystery key is sent as an input parameter and is then output as encrypted and BMP picture for the sender. This approach is called IDEA (International Data Encryption Algorithm) algorithm.

Aditya, Abhijeet, Hitesh & Rohan (2019) proposed a new approach in secure data stored on the cloud using a multiple cryptography algorithm and steganography. The 3DES (Triple Data Encryption Standard), RC6 (Rivest Cipher 6) and AES algorithms were used which provide the security of large data stored in the cloud. It was mentioned that the entire algorithm uses 128-bit keys.

3. METHODOLOGY

Security of data and file always pose a primary and pressing issue in cloud computing. The major concern of this work is to secure user data in the cloud during upload and download of data using Steganography and Cryptography and then evaluate the performance of the system. The steps used in this work to achieve the security of data in the cloud is by first conceal the data using image steganography and then cryptography to convert the data into a scrambled form that cannot be understood by an unauthorized user using DES encryption algorithm public key, and finally provide authentication to the data using DES private key. Application is deployed using the necessary algorithm to solve the problem of data thefts and unauthorized users to have access to the data in the cloud. Figure 1 depicts the system architecture of the proposed approach.

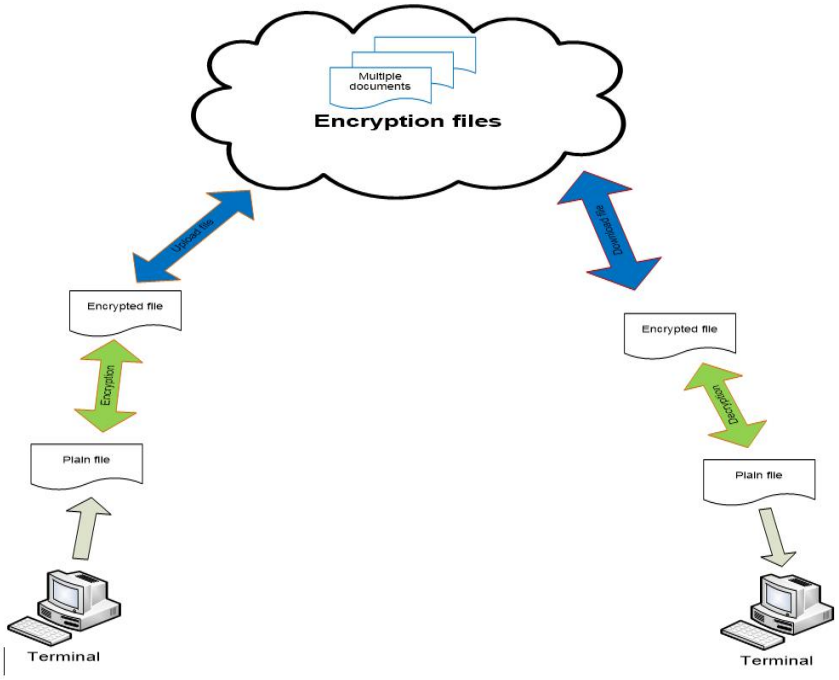


Figure 1: Proposed System Architecture

3.1 Steganography Layer

In this stage, two inputs are provided to the LSB steganography algorithm. The cover image is the first input, where the secret message or data is embedded into; and the second input is the secret message or data itself. The output of this stage is Stego Image that is, an image which contains secret information.

The Steganography layer in this study employs the Least Significant Bit (LSB) image steganography algorithm. When the message bit M_S of secret message to be embedded, is equal to the LSB of the pixel value of cover image $I_c(i, j)$, the bit remain unchanged; otherwise, set the LSB of I_c (i, j) to M_S. The message embedding Procedure is given below:

$SI(I, j) = I_c (i, j)$, if $LSB(I_c (i, j)) = M_S$; otherwise

$SI(i, j) = I_c (i, j) - 1$, if $LSB(I_c (i, j)) = 1$ and $M_S = 0$

$SI(i, j) = I_c (i, j) + 1$, if $LSB(I_c (i, j)) = 0$ and $M_S = 1$

where $LSB(I_c (i, j))$ represents LSB of cover image $I_c(i, j)$ and M_S is the subsequent message bit to be embedded. SI(i, j) is the stego image. The simple process of LSB algorithm is briefly described by a case of hiding alphabet "W" which ASCII code representation is 87 with the binary form of 1010111. These binary bits are embedded into LSB of Pixel value (Px). let consider three-pixel values as follows:

Pixels before Embedding:

Px 1: 10001100 01001111 01010100
Px 2: 00001111 11010101 11011010
Px 3: 11101000 11110110 10000001

Pixels after Embedding "1010111", *i.e.,* alphabet "W" using LSB Algorithm:

Px 1: 1000110**1** 0100111**0** 0101010**1**
Px 2: 0000111**0** 11010101 1101101**1**
Px 3: 1110100**1** 11110110 10000001

In the case above only six bits changed out of nine bits. This depends on the secret message to be embedded in the cover image.

Digital images have two categories, based on the number of bits that is, 8 bits and 24 bits. In the image of 8 bits, one bit of information can only be embedded. While in the image of 24 bits image, three bits of information can be embedded in each pixel as demonstrated in the case above. A picture of 800×600 resolution can accommodate about 144,000 bits of embedded data (Singh & Attri, 2015). Replacing the LSB of each pixel did not affect the appearance of the original image and therefore the Stego-image appears quite similar to the cover image.

3.2 Data Encryption Standard

The second layer of this work is the Data Encryption Standard (DES). The Stego image which contained embedded hidden message is the output of the first layer and served as input to the second layer where we encrypt the stego image with DES algorithm.

DES is a block cypher symmetric encryption algorithm with the key size of 64-bit. It was the first encryption algorithm developed by IBM and accepted for use by America National Institute of Standard and Technology (NIST) in 1977. DES algorithms used only 56-bits of it is data for encryption and the remaining 8-bits is used for error detection. It encrypts plaintext of 64-bits into a ciphertext of 64-bits using private key or subkey of 56-bits, the private keys were created from public keys of 64-bits long. The DES algorithm result produced 8 blocks of ciphers that were later merged into one ciphertext. Figure 2 shows the pseudocode of the DES algorithm. In the encryption phase, the public key generated algorithm is used to sign the document, while in decryption, the private key is used to verified and decrypt the file.

Start

Step:

1. DES accepts an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and produces an output of the 64-bit block.

2. The plain text block has to shift the bits around.

3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.

4. The plain text and key will be processed by the following:

a. The key is split into two 28 halves

b. Each half of the key is shifted (rotated) by one or two bits, depending on the round.

c. The halves are recombined and subject to a compression permutation to reduce the key from 56-bits to 48-bits. This compressed keys used to encrypt this round's plaintext block.

d. The rotated key halves from step 2 are used in the next round.

e. The data block is split into two 32-bit halves.

f. One half is subject to an expansion permutation to increase its size to 48 bits.

g. The output of step 4f is exclusive-OR'ed with the 48-bit compressed key from step 4c.

h. The output of step 4g is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.

i. The output of step 4h is subject to a P-box to permute the bits.

j. The output from the P-box is exclusive-OR'ed with other half of the data block.

k. The two data halves are swapped and become the next round's input.

End.

Figure 2: Pseudocode of DES Algorithm

Figure 3 and 4 show the flowchart details of the steps involved in uploading and downloading files from the cloud and a brief explanation of these step were provided below:

3.3 Encryption and Upload Stage

This is the stage where encryption of files or documents is performed and uploaded in the cloud. Figure 3 depicts the processes involved.

Prepared File: This refers to the preparation of the original file format at the sender end, the file is, therefore, in a format that the user prefers it to be without been seen by anybody during upload to the cloud except otherwise as preferred by the original owner of such files.

Steganography Module: This module uses Image Steganography to conceal the data to achieve a smooth transfer of data without drawing the attention of intruders to have access to the concealed information.

Cryptography module: This module encrypts the file using DES algorithm by converting it to a format that cannot be understood by intruders (cipher).

Encrypt and Upload: In this step, the user (sender) ensures that the necessary security on the file has been performed before it is uploaded to the cloud.

3.4 Decryption and Download Stages

This stage involved the steps of downloading the files from the cloud, decrypt and access the files. Figure 4 depicts the steps involved.

Download Decrypted: In this step, the decrypted file is download for the user to view and has access to the file.

Download Encrypted: In a situation whereby an intruder tries to access the file and the wrong key is entered the file that will be downloaded will be an encrypted file hence preventing the intruder from accessing the file.

View Encrypted File: In this step, when an unauthorized user enters the wrong key, the encrypted file is viewed but unable to decrypt or access the content of the file.

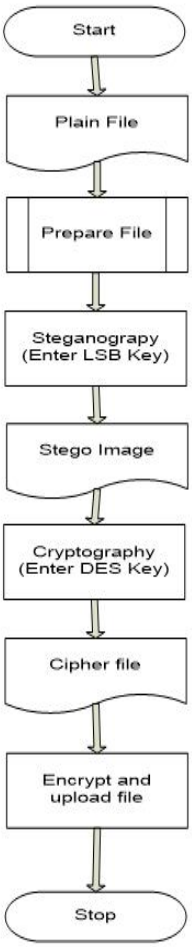


Figure 3: Flowchart of Encryption File

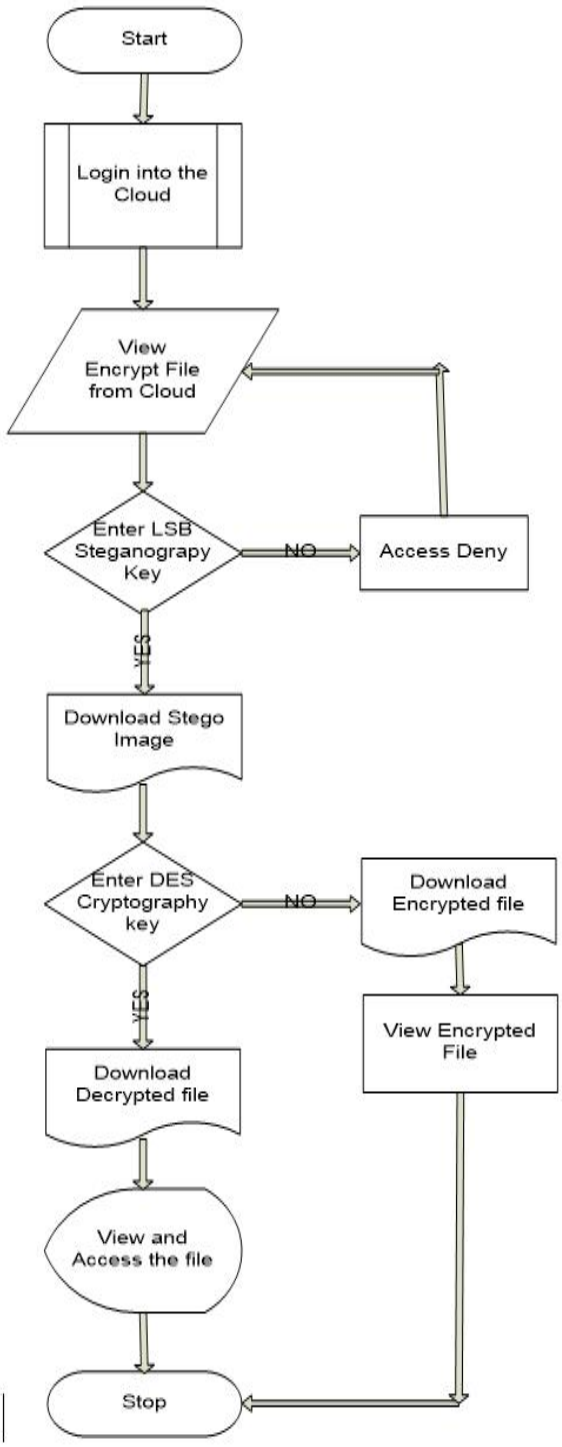


Figure 4: Flowchart of Decrypted File from the Cloud

4. RESULT AND DISCUSSION

The system was implemented and tested over a web browser on a live server.

Home page

The home page (Figure 5) is the first page on the system, it presents the user with a link to the login page and also with a link to create a new account for the new users.

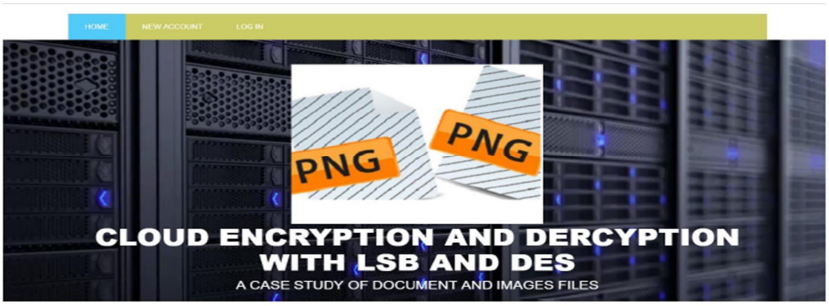


Figure 5: Index Page

Login page

On clicking the login link on the index page, the login page loads and the user can enter his or her email and password registered on the platform before. Figure 6 shows the sample. This page serve as medium of authentication and access into the system.

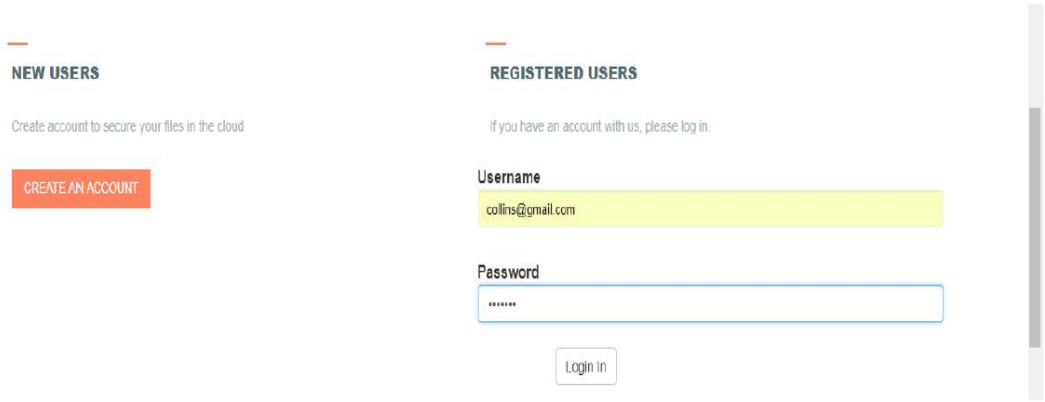


Figure 6: Login Page

New User Registration Page

The New User Registration page allows the new users to register on the platform by providing his/her details and password that will be used to access the platform.

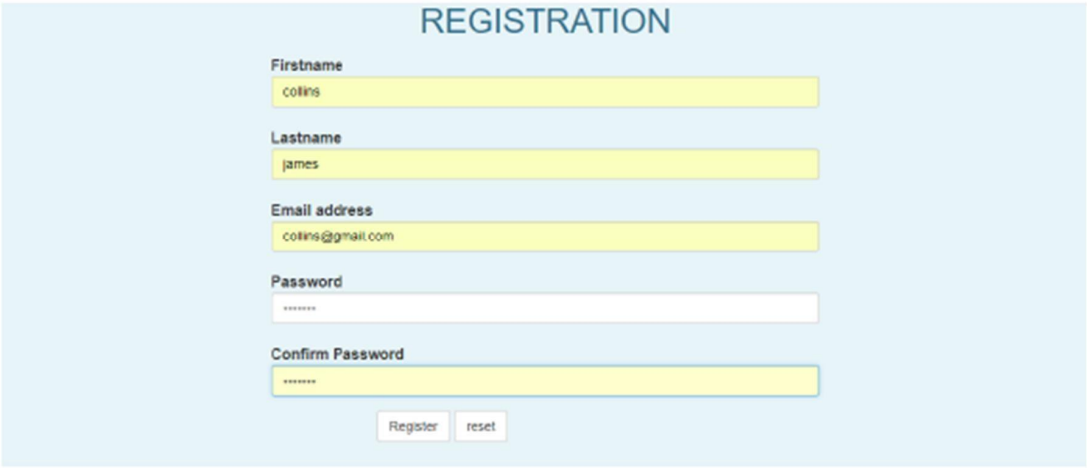


Figure 7: New User Registration

Uploading Files

Figure 8 shows the processing page of uploading a new file to the cloud, a name is given to the document which can be any image format, Word or pdf files, the LSB and DES public key is supplied to the appropriate field for the file encryption and hiding of the file with LSB Steganography.

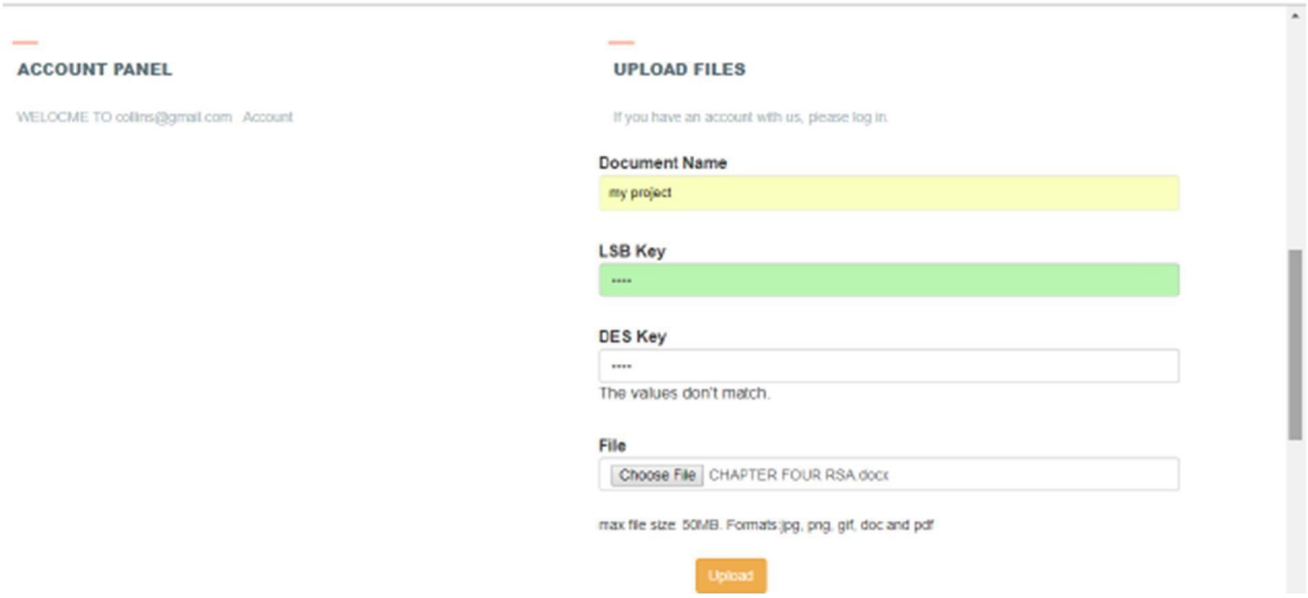


Figure 8: Uploading Files.

Cloud File List

The Cloud file list (Figure 9) shows the list of the encrypted files already stored in the cloud with the name of the files and the user account that uploaded the file.

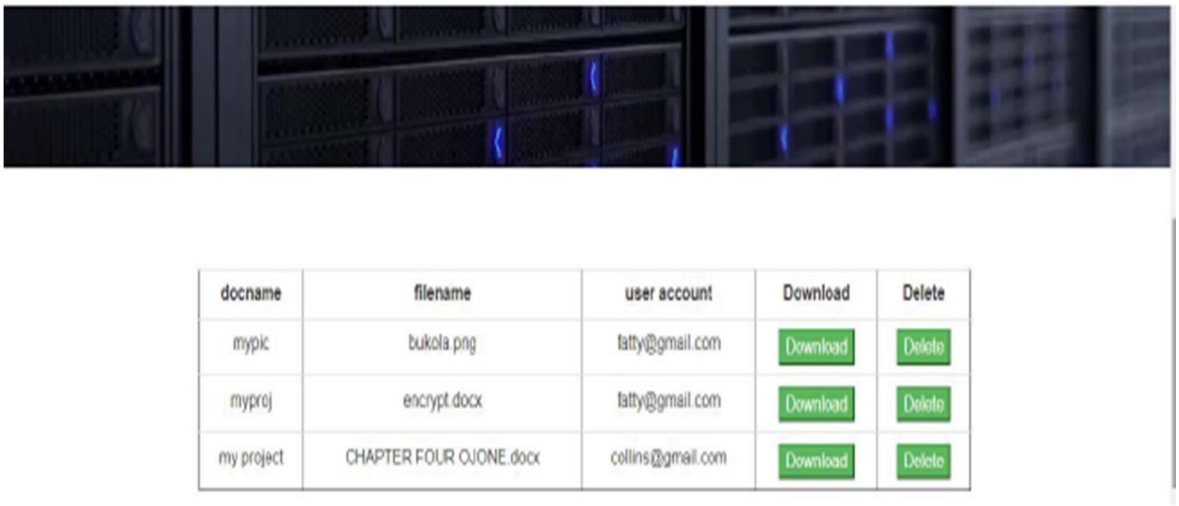
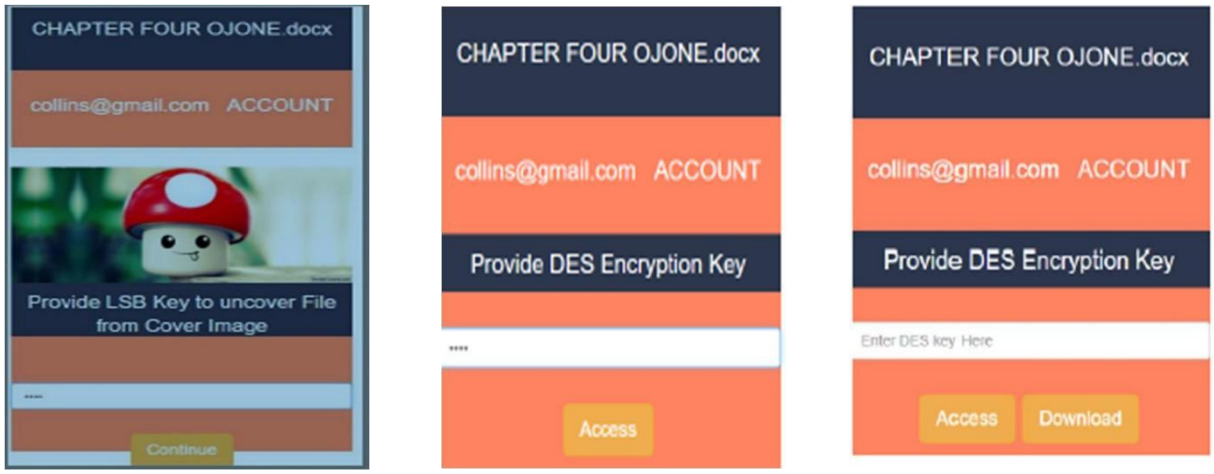


Figure 9: Cloud Files List

LSB User Authentication on cloud

Figure 10a shows the first stage of authentication with the LSB Steganography approach when the user wants to access the file in the cloud. After successful submission of the correct key, the page then navigates to the next layer of security which is DES Decryption process.



(a) (b) (c)

Figure 10: (a) LSB User Authentication. (b) DES User Authentication. (c) Download Access

DES User Authentication on cloud

Figure 10b shows the second layer of authentication with the DES Symmetric approach. Once the key is provided, it provides access to the download link.

Download Access page

Figure 10c shows the revealed download button for the user to download the file whether the DES keys are correct or incorrect. The download button will get the file from the cloud archive.

Download File List

Figure 11 shows the list of files stored in the cloud before for the users to download.

Name	Date modified	Type	Size
chap2 (1).docx	13-Apr-18 11:54 PM	Microsoft Word D...	224 KB
chap2 (2).docx	13-Apr-18 11:55 PM	Microsoft Word D...	224 KB
chap2 (3).docx	13-Apr-18 11:56 PM	Microsoft Word D...	224 KB
chap2.docx	13-Apr-18 11:54 PM	Microsoft Word D...	224 KB
CHAPTER FOUR OJONE (1).docx	19-Jun-18 8:26 AM	Microsoft Word D...	1,849 KB
CHAPTER FOUR OJONE (2).docx	19-Jun-18 8:26 AM	Microsoft Word D...	1,849 KB
CHAPTER FOUR OJONE (3).docx	19-Jun-18 8:29 AM	Microsoft Word D...	1,849 KB
CHAPTER FOUR OJONE.docx	19-Jun-18 8:24 AM	Microsoft Word D...	1,849 KB
chapter two muji.docx	13-Apr-18 11:48 PM	Microsoft Word D...	239 KB

Figure 11: List of Files in the Cloud

Figure 12 shows the document opened when the correct DES key was supplied by the user thereby decrypt and giving the user access to the contents of the file.

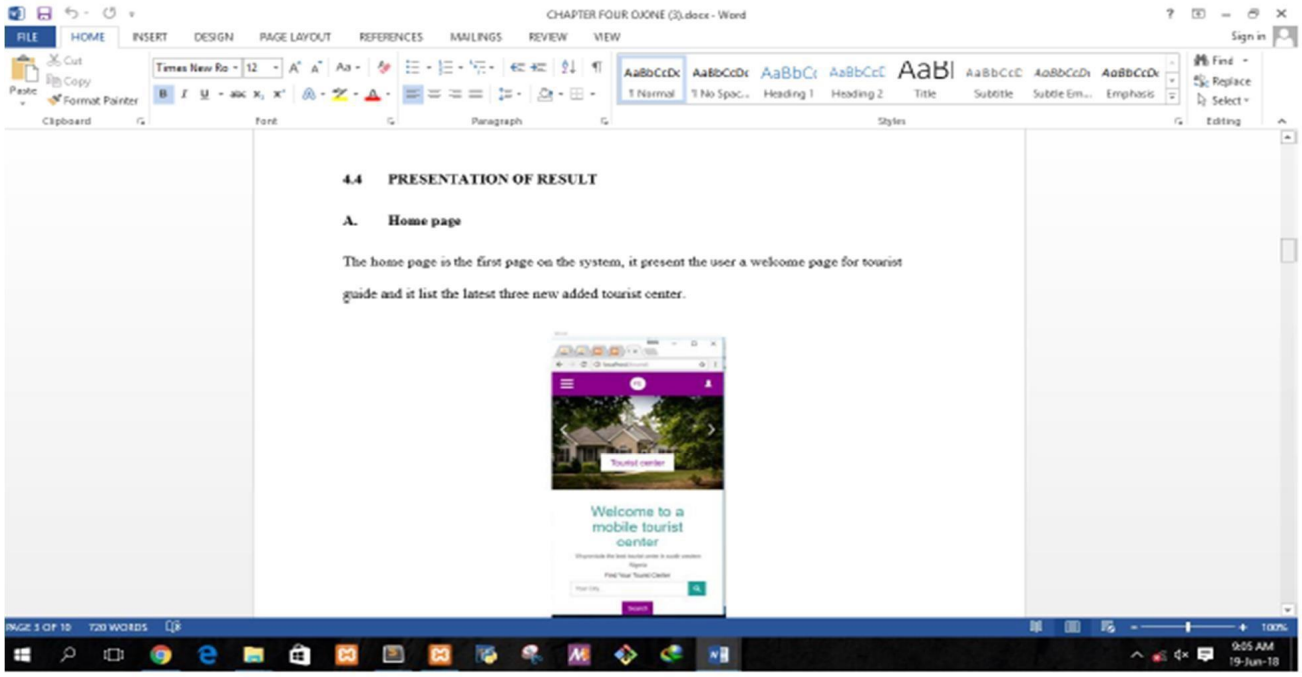


Figure 12: Decrypted File

However, when the wrong DES Key entered, the encrypted file (Figure 13) is displayed to deny unauthorized user access to the content of the file.

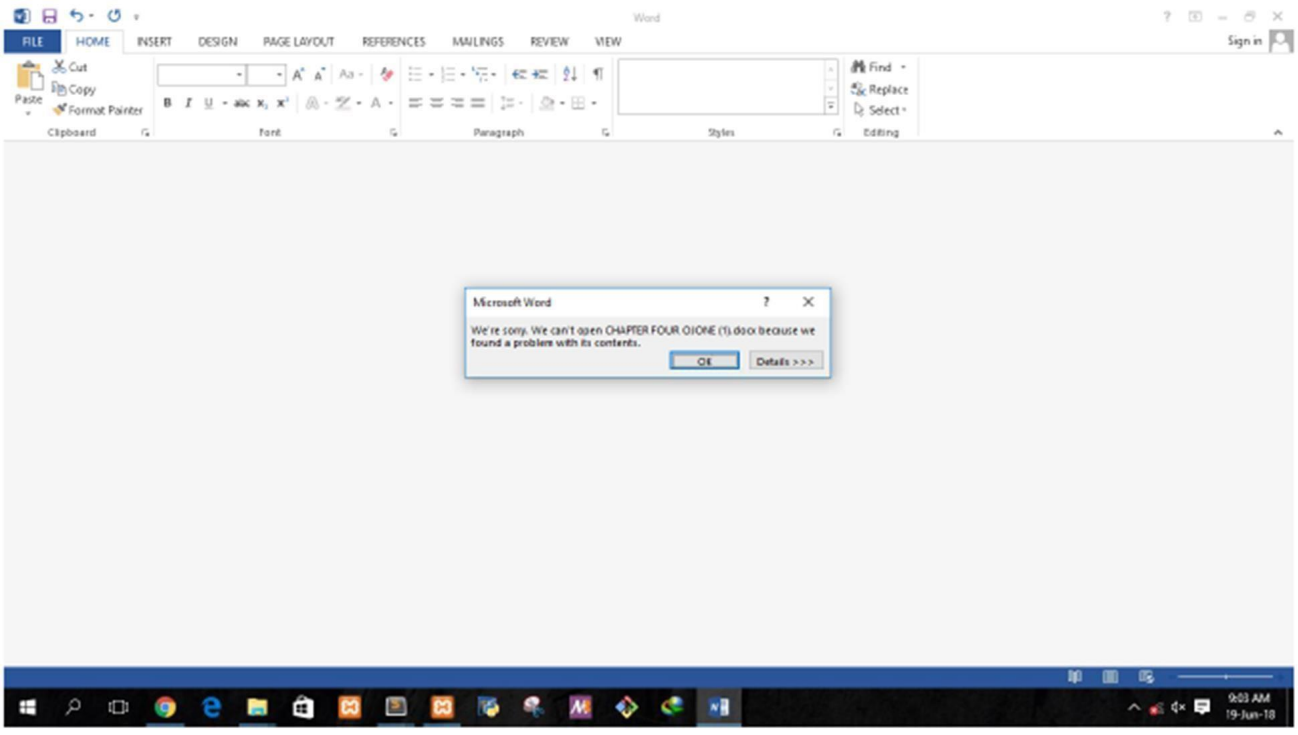


Figure 13: Encrypted File

5. CONCLUSION AND FUTURE WORK

This study presented a twofold layer of security, that is, the combination of LSB steganography image encoding approach and DES cryptography encryption technique to improve the security of data in the cloud. The mayhem caused by cyber hacker or thief on the documents stored in the cloud motivates this research to implement a double layer security system. The results of this work revealed that a dual security layers system provide extra security power and make cyber-attack to be a more challenging task to be accomplished. This work was able to secure document files in Word document and pdf as well as images files.
In the future, we will try to combine two cryptography techniques to make a brutal attack to be more difficult and also extend our work to video and audio files.

REFERENCE

[1] Adamu, I. A., & Boukari, S. (2017). An Enhanced Cloud-Based Security Using RSA as Digital Signature and Image Steganography. *International of Scientific and Engineering Research, 8*(7).

[2] Aditya, P., Abhijeet, D., Hitesh, N., & Rohan, N. (2019). Secure File Storage on Cloud using Hybrid Cryptography. *International Journal of Computer Sciences and Engineering, 7*(1), 587-591.

[3] Ahmed, A.-S., & Talal, A. (2017). Cryptography and Steganography: New Approach. *Transactions on Networks and communications, 5*(1), 2533.

[4] Ahmed, U. Z. (2018). Security during Transmission of Data Using Web Steganography. *Culminating Projects in Information Assurance*, M. Sc. Thesis, St. Cloud State University.

[5] Aiswarya, B., & Hema, K. (2017). Combined Strength of Steganography and Cryptography-A Literature Survey. *International Journal of Advanced Research in Computer Science, 8*(3), 1003-1010.

[6] Arockiam, L., & Monikandan, S. (2013). Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(8), 3064-3070.

[7] Babatunde, A. O., Taiwo, A. J., & Dada, E. G. (2018). Information Security in Health Care Centre Using Cryptography and Steganography. *arXiv preprint arXiv:1803.05593*.

[8] Basri, M., Mawengkang, H., & Zamzami, E. M. (2018). Cloud Computing Security Model with Combination of Data Encryption Standard Algorithm (DES) and Least Significant Bit (LSB). *Journal of Physics: Conference Series*, 1-7.

[9] Sasikumar, V., & Vijayanandh, R. (2017). Secure Steganography Methodology using Combined Encryption and Quick Response Codes. *International Journal of Latest Trends in Engineering and Technology, 8*(1), 486-493.

[10] Kaur M. & Singh H. (2015). A Review of Cloud Computing Security Issues *International Journal of Advances in Engineering & Technology (IJAET),* 397-403.

[11] Marwa, E. S., Abdelmgeid, A. A., & Fatma, A. O. (2016). Data Security using Cryptography and Steganography Techniques. *International Journal of Advanced Computer Science and Applications, 7*(6), 390-397.

[12] Mathew S (2012). Implementation of Cloud Computing in Education - A Revolution *International Journal of Computer Theory and Engineering,* 473-475.

[13] Nancy G., & Kamalinder K., (2016). Data Storage Security using Steganography Techniques, International Journal of Technical Research and Applications, 4 (6), 93-98.

[14] Ngatia, E., & Njuguna, A. (2018). Information Security through an Improved Image Steganography Algorithm. *Journal of Information and Technology, 1*(1), 28-46.

[15] Omer, K. J., Safia, A., El-Sayed, M. E.-H., & Abdel-Badeh, M. S. (2013). Efficiency of Modern Encryption algorithms in Cloud Computing. *International Journal of Technology in Computer Science, 2*(6), 1-8.
[16] Ravi Kumar. B. & Murti. P.R.K. (2011). Data Security and Authentication using Steganography. International Journal of Computer Science and Information Technologies (IJCSIT), 2(4), 253-256.
[17] Satwinder, S., & Varinder, K. A. (2015). Dual Layer Security of Data using LSB Image Steganography Method and AES Encryption Algorithm. *International Journal of Signal Processing, 8*(5), 259-266.
[18] Singh S. & Attri V. A. (2015). Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm, International Journal of Signal Processing, Image Processing and Pattern Recognition 8 (5), 259-266.
[19] Vinita, K., Ali, S., & Sharma, N. (2016). Hybrid Approach of Cryptographic Algorithm in Cloud Computing. *International Journal Emerging Technology* and Advanced Engineering, 6 (7), 87-90.

Article received: 2020-03-16