Cloud Computing Security Model with Combination of Data Encryption Standard Algorithm (DES) and Least Significant Bit (LSB)

M Basri, H Mawengkang, E M Zamzami

1Department of Computer Science, Faculty of Computer Science and Information Technology, University of Sumatera Utara, Jl. Universitas No. 9-A, Medan 20155, Indonesia.

*Email: mhdbasri@unimed.ac.id, hmawengkang@yahoo.com, elvi_zamzami@usu.ac.id

Abstract. Limitations of storage sources is one option to switch to cloud storage. Confidentiality and security of data stored on the cloud is very important. To keep up the confidentiality and security of such data can be done one of them by using cryptography techniques. Data Encryption Standard (DES) is one of the block cipher algorithms used as standard symmetric encryption algorithm. This DES will produce 8 blocks of ciphers combined into one ciphertext, but the ciphertext are weak against brute force attacks. Therefore, the last 8 block cipher will be converted into 8 random images using Least Significant Bit (LSB) algorithm which later draws the result of cipher of DES algorithm to be merged into one.

1. Introduction

Cloud computing is a metaphor of a computer / internet network that is abstracted from a concealed complex infrastructure [1] that enables one to store, change and even create applications within a virtual server owned by a cloud computing service provider. Cloud computing is basically in use for the file can be accessed anywhere and gated not in one device only. Cloud computing allows users to get access to various computing resources in a simple, periodical, efficient storage space, as well as software applications, for access to all it requires only browser applications [2]. However, some threats such as data theft known as breach / loss data [3] may occur. Therefore cloud computing as well as storing data freely but also pay attention to privacy security as the most important priority.

Attack of security loopholes using man in the middle attack (MitM) technique when sending data to cloud storage. MitM attacks are a type of attack that makes it seem that two legitimate users are communicating with each other, but there is somebody between them who sends and receives data from both users [4]. As for other attacks after obtaining user and system cloud password by using social engineering or Man-in-the-Middle Attack is by using attack on file encryption side [5]. MitM can be prevented by securing data using cryptography. However, cryptographic encryption techniques can also be attacked using cryptanalysis attacks that predict the algorithm used for message encryption. To prevent this is necessary steganography techniques.

Data Encryption Standard (DES) included into the cryptographic system symmetry and belonging to the type of block cipher. DES operates on 64-bit block size. DES encrypts 64 bits
of plaintext into 64 bits of ciphertext using 56 bits of internal key or subkey, internal keys generated from external keys 64-bits long [6]. The result of this DES algorithm will produce 8 blocks of ciphers which will then be merged into one ciphertext, but the ciphertext is weak against the brute force attack, therefore the last 8 block cipher will be converted into 8 random images using the Least Significant Bit algorithm (LSB) which later the image of DES algorithm cipher result will be merged into one.

Theoretically Least significant Bit (LSB) conceals messages secretly by replacing the data bits in the image segment with bits of secret messages. These lowest bits will then be inserted into the lowest bit or the far right bits in the pixel of the drawing composed of red, green and blue (RGB) each having an 8 bit value of 0 to 255 with binary form 00000000 to 11111111. 3 bit data can be inserted in each available image pixel. The LSB method is then applied in a library which is then named as a stagger that has a function to insert messages into images.

2. Method

Cloud security model created using PHP running localhost and online on windows operating system 10. This model will be made into the process of cloud computing where a file that will be sent to the cloud will do the encryption process so that the file will be a cipher while in the cloud storage. At the time of retrieving the file, then the file will go through the decryption process, if the key for decryption is correct then the file will be changed to plain. Illustration of the above model can be seen in the following figure 1 and 2.

![Figure 1. Design of security models.](image1.png)

![Figure 2. Design of security models in the cloud.](image2.png)

When the file process (figure 2) uploaded into the cloud storage file will be processed by the DES algorithm, the original file will be split into conversions into binary numbers then the result of the bits is merged into one called plaintbit and will be processed together with the bits of the key. The results of this plaintbit will then be randomized by using Initial Permutation (IP) and will go through a randomization process that will make the IP into 8 parts that each part is done 16 times the rotation process. The result of this rotation process will result in PlainBit IP.

Each PlainBit IP generated by the DES algorithm will then be processed using the LSB algorithm, then every bit processed with the LSB algorithm will be made into one in an image to be inserted, in this model the process of the DES algorithm is not completely working on the file but when the DES algorithm proceeds to the result of PlainBit IP then the result will be directed to the LSB algorithm to overcome the weakness of DES algorithm from brute force attack.
2.1. Encryption process using DES algorithm

![DES flow diagram of DES encryption process.](image1)

The process of sending text and files will be encrypted using DES 16 round algorithm to generate cipher bits from each round. DES algorithm will do the calculation of plaintext and key. The steps of the DES 16 round algorithm can be seen in figure 3.

2.2. The process of inserting bits 16 round using LSB algorithm

![LSB algorithm flow diagram.](image2)

Each bit generated by 16 rounds on the DES algorithm will be inserted by using the LSB algorithm. This insertion process requires a master image / cover image. The bits will be inserted into R, G and B in the image by replacing the last bit in R, G and B so that the 16 round bits are inside the cover image. The insertion flow diagram of 16 round bits of DES can be seen in figure 4.
2.3. Decryption using LSB and DES algorithms

The decryption process is the process of returning plaintext from the cover image. Images generated by the LSB algorithm will be decrypted using keys to generate ciphertext. Ciphertext which is the output of each bit of R, G and B cover image on the LSB algorithm will generate 16-bit bits of the DES algorithm (in this process there needs to be an LSB conversion to the binary number). Chiperbit to be decrypted with bit key so it will generate cipherIPinvers, this process flow chart can be seen in figure 5 below.

![Figure 5. LSB decryption process flowchart.](image1)

![Figure 6. DES descriptor flow process diagram.](image2)

Next cipherIPinvers result from LSB decryption will be returned again into ASCII bit through 16 rounds of DES algorithm. The decryption flow diagram can be seen in Figure 6 above.

3. Result and Discussions

The results of this study is a model of the DES algorithm with a 16-round process to create a ciphertext. The 16-round process will then produce 16 parts, of which 16 parts are combined to produce a ciphertext. Ciphertext of DES algorithm has weakness in its security, as it is easy to attack cryptanalysis by using brute force algorithm. Therefore in this study the DES algorithm is not processed until the end becomes ciphertext.

At the time of 16 rounds occur then each of the 16 rounds will be inserted into an image with LSB algorithm so that the cover image. The LSB algorithm allows a message to be inserted into an image by replacing the smallest bit to hide the message. To perform the implementation of this research, the authors need to conduct trials and analysis.

The display of this trial program shown in figure 7 and 8. Figure 7 shows the login form of the cloud system application and figure 8 is the main menu display after login.
Figure 7. Cloud system login.

Figure 8. Form the insertion of images into the cloud.

3.1. Cloud security model of text / file encryption process
The first experiment will be the process of selecting the image of the host or the image to be inserted by the DES algorithm process using the LSB algorithm as in figure 9 above. Then select the text menu / file for the calculation process in the DES algorithm that will be inserted into the host image that has been uploaded before. Then save the encryption result in figure 10 into the host image so that this encryption result is not visible. The host image will be saved into the cloud and can not be downloaded by anyone who can not access permissions. Figure 11 is a view of the host image that has been automatically uploaded to the cloud system after passing the DES 16 round and LSB algorithm.

Figure 9. The host image to which the text will be inserted.

Figure 10. Text message encryption process.
3.2. Cloud security model of text / file decryption process

After going through the process of cloud computing security, the image file will be in the cloud. Users can share files that are in the cloud by sharing the link of available files, but to see the hidden messages in the image it must do the decryption first. The decryption process can be seen in figure 12. Figure 13 is the process of decrypting a successful text message.

Figure 11. Images that have been saved in the cloud.

Figure 12. The image to be decrypted

Figure 13. Text message decryption process succeeded.

Figure 14. Text message decryption failed

Figure 15. The file decryption process failed.
Figure 14 is a picture of a failed text message process and picture 15 is a picture on the decryption process the key entered is not the same as the key at the time of encryption then the decryption process will occur failure and the file can not be downloaded.

4. Conclusions

The conclusions of this study are as follows. First, cloud computing security model used in file and message storage processes requires the DES cryptography algorithm and LSB steganography in the 16th round of bits to keep up the security and confidentiality of files and messages. Second, process of validating files and messages that will be downloaded using the cloud computing security model if the key does not match then the file will not be downloadable.

References

[1] N A S and Hemalatha M 2012 Cloud Computing for Academic Environment International Journal of Information and Communication Technology Research 97-101
[2] Mathew S 2012 Implementation of Cloud Computing in Education - A Revolution International Journal of Computer Theory and Engineering 473-475
[3] Kaur M and Singh H 2015 A Review Of Cloud Computing Security Issues International Journal of Advances in Engineering & Technology (IJAET) 397-403
[4] Gaikwad B P 2014 A Critical Review on Risk of Cloud Computing in Commercial International Journal of Innovative Research in Computer and Communication Engineering 1-8
[5] Ahmed E S and A Saeed R 2014 A Survey of Big Data Cloud Computing Security International Journal of Computer Science and Software Engineering (IJC SSE) 78-85
[6] Kaur N and Sodhi S 2016 Data Encryption Standard Algorithm (DES) for Secure Data Transmission International Conference on Advances in Emerging Technology (ICAET) 31-37