ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A TECHNIQUE TO INCREASE INTEGRITY OF CLOUD DATA USING HYBRID ALGORITHMS

Ms. Manisha*, Dr. Kamlesh sahrma, Ridhika Sharma

ABSTRACT

Cloud computing is an internet based modern technique, which is capable of providing us various resources. The availability of these resources are very flexible in nature i.e. few are available to customers free of cost but some on a pay as use basis. Along with this the customer is also allowed to access information and can utilize computer resources from anywhere if having the internet access. Various security issues, like hacking, stealing, unauthorized access etc. are also emerging along with the emergence of the same. These security related issues degrade the popularity of cloud computing. To overcome these issues, we are using SHA 512, AES, and Steganography.

KEYWORDS: Cloud computing, SHA512, Steganography, AES. Introduction (Heading 1)

INTRODUCTION

Cloud computing is a hub of various servers and many database to store data. In other words, cloud computing is a term which is used to refer a model of network computing where a program or application runs on a connected server or servers rather than on a local computing devices such as PC, like the traditional client-server model. It is an internet based technology in which data security becomes a big issue to the cloud data [3]. The main shortcoming linked to this technology is that user do not have any ideas of where their data is kept and who manages their data. Cloud computing customers do not own the physical infrastructure rather they only use certain amount of space on that cloud computing service provided by the third party [4].Our scheme uses a light weight front end server to connect all request with name modes-Triple security[5].

SHA-512

The National institute of standard and technology (NIST) along with NSA developed the secure hash algorithm. SHA works with any input message that is less than 264 bits in length. The output of SHA is a message digest, which is 160 bits in length. In 2002, NIST had come up with a new version of SHA in standard document FIPS 1802, called SHA-256, SHA-284, SHA-512; with the number after the word SHA indicating the length of the message digest in bits. The SHA-512 algorithm takes a message of length 2128bits, and produces a message digest of size 512 bits. The input is divided into blocks of size 1024 bits each [1]. Shay gueron, simon Johnson, jesse walker shows the comparison of SHA-512 and SHA-256. Hashing algorithms considered as a poor man of the community, with their security receiving less attention than standard encryption algorithms and with little attention paid to their speed also. This resulted in shifting of many standards and products towards larger hash sizes. The reason why SHA-512 is faster than SHA-256 on 64 –bit machines is that it has 37.5% less rounds per byte (80 rounds operating on 128 byte blocks) compared to SHA-256[4].

AES

The AES also referenced as Rijndael (its original name), which is a specification for the encryption of electronic data established by the U.S (NIST) in 2001. AES has also been adopted by the U.S government and now has worldwide acceptance. AES is developed by two Belgium cryptographers, Joan Daemon and Vincet Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different keys and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key length 128, 192, 256 bits [2]. Weaknesses in DES created the need to come up with this new algorithm. DES were based on 56 bit key and 64 bit blocks and thus considered weak. AES was to be based on 128-bit blocks with 128-bit keys. The key length and the length of the plain text blocks need to be selected independently and hence AES emerged. Rijndael also uses the basic techniques of substitution and transposition (i.e. permutation). The key size and the plain

text block size decide how many rounds need to be execute the minimum no. of rounds is 10 and the maximum no. of rounds is 14[1].

STEGANOGRAPHY

It is the art and science of writing hidden messages in such a way that no one else apart from the intended recipient knows the existence of the message. This technology in network security use to hide the message behind an audio, text, object and image. Applying this technology enables message to be read by the sender and receiver only and protects the privacy of the message and also prevents unauthorized access. Cover objects refers to the text file, audio file, video files and Images in which the message is to embed in steganography technique. There are different methods used in steganography such as [9]:

1. Hiding message behind text file.
2. Hiding message behind an image.
3. Hiding message behind an audio file.
4. Hiding message behind an audio file.
5. Hiding message behind video file.

In this paper we will emphasize on explaining the techniques under the point 1 and 2 of above stated list.

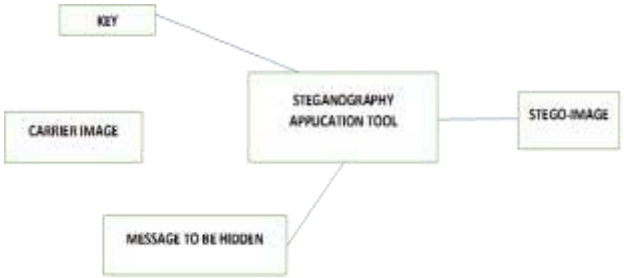
Audio Steganography: In a computer based audio steganography system, secret message are embedded in digital sound. Slight alteration in the binary sequence of a sound file is done to embed the secret message. Existing audio steganography software can embed message in WAV, AU, and even MP3 sound file [6].

Image Steganography: Images are the most popular cover objects for steganography where an altered image with slight variations in its colors will occur but is almost indistinguishable from the original image when observed by a person. This reveals the importance of image steganography. The basic structure of image steganography is made up of three components:

1. Carrier Image
2. The message.
3. The key.

The carrier can be a painting, or a digital image.it is the object that will carry the hidden message. A key is used to decode/decipher the hidden message. This can be anything from a password, a pattern.

Figure 1:



Block Diagram of Image Steganography

Steganography is achieved by LSB (LEAST SIGNIFICANT BIT TECHNIQUE).

LSB (LEAST SIGNIFICANT BIT TECHNIQUE): The least significant bit is one of the main technique in image steganography [7].Least Significant bit insertion is a common and simple approach to embed information in the image file.

ALGORITHM [8]

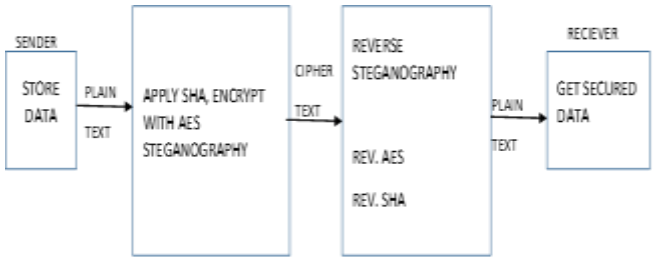
1. Select a cover image of size M*N as a input.
2. The message to be hidden is embedded in RGB component only of an image.

3. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate.The filter is also applied to least significant bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).
4. After that message is hidden using bit replacement method.

PROPOSED WORK

In our proposed work we provide security by implementing three algorithms SHA-512, AES and steganography together to secure data. To implement these three algorithm we use visual studio as a platform.

Figure 2:



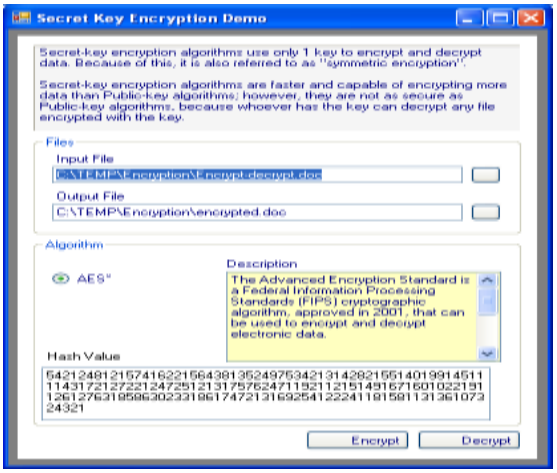
System Design of Proposed Work

RESULT ANALYSIS: SNAPSHOTS

Figure:

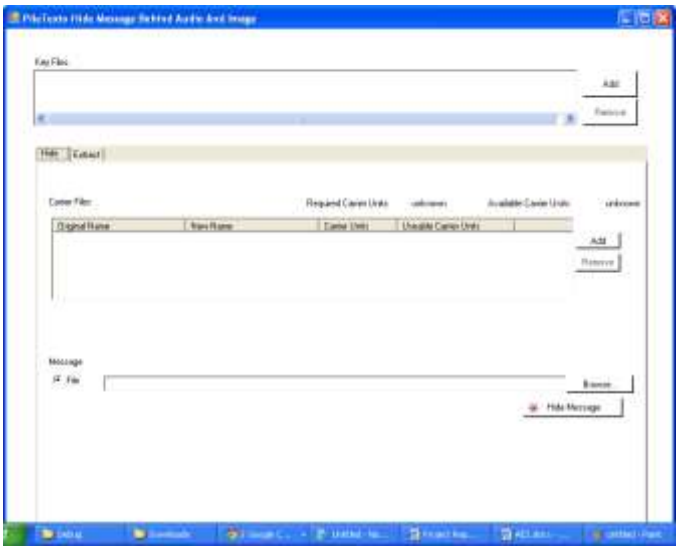
SHA-512

Figure:



AES

Figure:



STEGANOGRAPHY

HARDWARE & SOFTWARE REQUIREMENTS

➢ Hardware Used

- One computer with 2 GB of memory
- 80 GB hard disk space
- An Intel Pentium Core 2 Duo based computer working at least @ 2.2 GHz speed
- 17 inch monitor

➢ Software Used

- Microsoft Visual Studio 2008
- Windows XP operating system
- MS-office

CONCLUSION

In our proposed system, SHA-512 is used for verify integrity of data. For encryption, we use AES and then apply Steganography which can change presentation of data so that unauthorized person could not access the hidden data. Hence this is essential for providing maximum security to the data. Receiver can get original plain text by reversing the, SHA-512, AES, steganography.

Future Work: In this paper, we implemented SHA-512, AES and STEGANOGRAPHY to provide maximum security in cloud computing. By implementing these three algorithm we are intended to provide maximum security to the data. The technique used also increased the time complexity which should be reduced and hence we will try to improve the same.

REFERENCES

[1] Atul Kahate,"Cryptography and Networking Security",3ed.
[2] http:// en,wikepedia.org/wiki/Advanced-encryption-standard.
[3] Garima Saini1, Naveen Sharma2 "Triple Security of Data in Cloud Computing, IJCSIT, Volume No.5(4), 2014 5825-5827, ISSN: 0975-9646.
[4] Parul Mukhi1, Bhawna Chauhan2, Triple Security in Cloud Computing, International Journal Of Engineering and Computer Science, Volume no.3, Issue 7, July, 2014, Page no.7364-7374, ISSN:2319-7242.
[5] Parul Mukhi1, Bhawna Chauhan2, "Survey On Triple Security in Cloud Computing" IJCSMC, Vol. no. 3, Issue, 4, April 2014, pg.1108-1115, ISSN 2320-088X.

[6] Tomar Kuldeep1, Arya Richa2, "Triple Security of File System of Cloud Computing", IJRASET, Vol. no. 2, Issue I, January 2014, ISSN: 2321-9653.
[7] Champakamala1, B.S. Padmini.k2 et.al "Least Significant Bit Algorithm for image Steganography", IJACT, ISSN: 2319-7900.
[8] Shilpi Gupta1, Geeta Gujral2 et.al "Enhanced Least Significant Bit algorithm for Image Steganography", IJCEM, Vol. no. 15,ISSUE 4, July 2012, ISSN(Online) 2230-7893.
[9] Khushboo Gupta1, Neha Goyal2, et.al "Study of Security algorithm to Provide Triple Security in Cloud Computing", International Journal of Scientific and Research Publication,", Volume 4, ISSUE 6, June2014.