ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Enhancing Data Security for Cloud Environment based on AES Algorithm and Steganography Technique

G.Yogeswari [1], **P.Eswaran** [2]
[1] *M.Phil. Research Scholar,* [2]*Assistant Professor*
Department of Computer Science and Engineering, Alagappa University, Karaikudi, India
[1] yogifriends.share@gmail.com, [2]eswaranperumal@gmail.com

***Abstract*— The Cloud Computing is a peppy term, which provides hassle free data outsourcing facility which prevent the user from burdens of local storage issues. However, security is perceived as a biggest issue and poses new challenges related to providing secure and reliable data archive over unreliable service providers. In this paper, we proposed an elegant and novel method to enhance security aspects by associating cryptographic techniques along with Steganography. This paper offers confidence and trust by make use of improved dual key AES algorithm along with Steganography. From the theoretical and performance analysis, it shows that the proposed scheme is highly efficient and provably secure.**

***Keywords*— Cloud Computing, Security, Cryptography, Steganography, AES.**

I. INTRODUCTION

Cloud computing is a service provider which delivers software on demand and makes the users to access the resources remotely without any issues about the management and maintenance of resources dynamically[1].

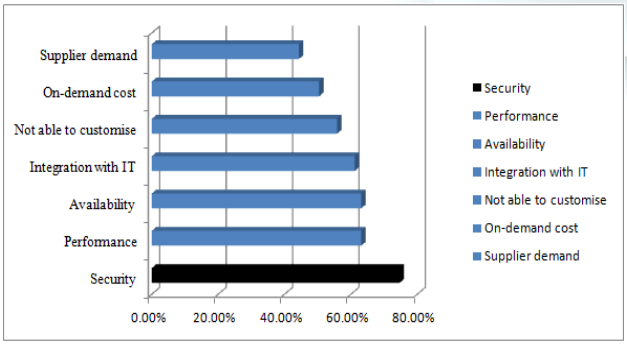


Fig. 1 Issues of Cloud Computing

Although cloud is a promising innovation with various benefits in the world of computing, it comes with certain risks. Security is the biggest concern about cloud computing represented in figure 1 [4, 5, 7, and 10]. In account of strengthening the communication efficiently, additional algorithms and data covering techniques should be applied to make the intruder unaware of passing secret data. Cryptography as well as Steganography are the two techniques that grasp data in order to hide their existence respectively. Steganography is a branch knowledge of communicating in a way which hides the existence of the views [6, 9, and 11]. Steganography is an origin of Greek term and essentially means covered writing.

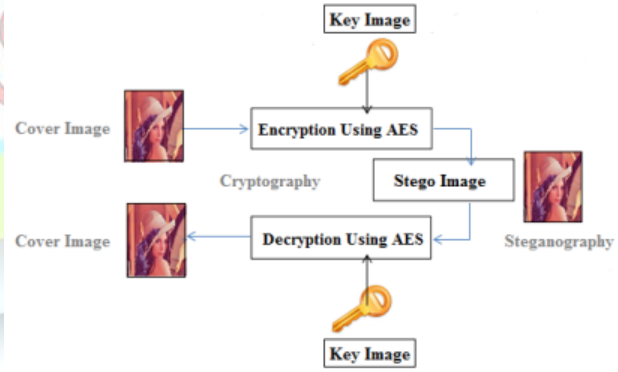


Fig. 2 Associating Cryptography and Steganography in Cloud Environment

Cryptography mish mash a message so it can be difficult to assume or perceive the message exactly. While steganography covers the data so it can be unseen. Although these methods provide individual security, a method is made to combine both the techniques into a system for even more security and confidentiality [2, 12]. Christo Ananth et al. [7] proposed a system which can achieve a higher throughput and higher energy efficiency. The S-BOX is designed by using Advanced Encryption Standard (AES). The AES is a symmetric key

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

standard for encryption and decryption of blocks of data. In encryption, the AES accepts a plaintext input, which is limited to 128 bits, and a key that can be specified to be 128 bits to generate the Cipher text. In decryption, the cipher text is converted to original one. By using this AES technique the original text is highly secured and the information is not broken by the intruder. From that, the design of S-BOX is used to protect the message and also achieve a high throughput, high energy efficiency and occupy less area.

The main aim is to denote a method for integrating secret and covered writing techniques together for a cloud environment which is represented in the figure 2. The secret data is embedded within the image called cover image. Cover image carrying embedded secret data is referred as stego image.

This paper organized into following sections. Section I describes the introduction part along with cryptography and steganography techniques. Subsequently section II described the advanced encryption standard algorithm. Traditional LSB Substitution technique is discussed in section III. In section IV related works are described in detail. Proposed works are explained in section V and experimental results in section VI. This paper concluded and mentioned its further enhancements in section VII.

II. ADVANCED ENCRYPTION STANDARD ALGORITHM

The Advanced Encryption Standard is a cryptographic algorithm and has four basic transformations; the key length may be 128, 192 or 256. In this research 128 bit key length is followed, AES breakdown data into matrix of bytes of predetermined size and encode every state independently [3, 8].They are represented as follows:

$$A = \begin{bmatrix} a(0,0) & a(0,1) & a(0,2) & a(0,3) \\ a(1,0) & a(1,1) & a(1,2) & a(1,3) \\ a(2,0) & a(2,1) & a(2,2) & a(2,3) \\ a(3,0) & a(3,1) & a(3,2) & a(3,3) \end{bmatrix}$$

The algorithm for AES consists of smaller, sub–algorithms namely SubBytes, ShiftRows, MixColums, and AddRoundKey, where each method will be explained below:

A. SubBytes

In subbytes each element, each byte in the matrix is replaced by using Rijndael's S-Box. This method is basically consists of two stages. Initially each byte is replaced with its multiplicative inverse. The final stage affine transformation is performed.

$$A.x+b \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x0 \\ x1 \\ x2 \\ x3 \\ x4 \\ x5 \\ x6 \\ x7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

The inverse affine transformation is as follows:

$$C.y+d \quad \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} y0 \\ y1 \\ y2 \\ y3 \\ y4 \\ y5 \\ y6 \\ y7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

B. ShiftRows

ShiftRows is the simplest operation to change the order of data.

$$A = \begin{bmatrix} a(0,0) & a(0,1) & a(0,2) & a(0,3) \\ a(1,0) & a(1,1) & a(1,2) & a(1,3) \\ a(2,0) & a(2,1) & a(2,2) & a(2,3) \\ a(3,0) & a(3,1) & a(3,2) & a(3,3) \end{bmatrix}$$

Then A' is given by:

$$A' = \begin{bmatrix} a(0,0) & a(0,1) & a(0,2) & a(0,3) \\ a(1,1) & a(1,2) & a(1,3) & a(1,0) \\ a(2,2) & a(2,3) & a(2,0) & a(2,1) \\ a(3,3) & a(3,0) & a(3,1) & a(3,2) \end{bmatrix}$$

C. MixColumns

The MixColumns messes with columns instead of rows and linear transformation is performed, it has an inverse, this operation is also invertible.

D. AddRoundKey

AddRoundKey is the final stage and this process consists of the following parts: Rotate, Rcon, and subbytes. The initial part is to rotate the bytes towards left, the next part is to apply sub-operation called Rcon, and the final part is to perform Rijndael's S-Box.

III. TRADITIONAL LSB STEGANOGRAPHY SUBSTITUTION

The traditional LSB substitution based on RGB color codes are used, LSB is based on spatial domain using intensity values of the pixels in each co-ordinate position. Here LSB of the cover image will be replaced with the secret message, plane of the image only be modified, and does not cause much distortion to the cover image, The three adjacent pixels of an image with RGB encoding:

00001101	00011101	11111001
10000110	00011111	11011010
10001111	00110000	11011011

Message to be hidden is of 9 bits, which is given by 101101101. Overwriting of 9 bits over the LSB of the 9 bytes above, the result will be:

00001101	00011100	11111001
10000111	00011110	11011011
10001111	00110000	11011011

Thus 9 bits are hidden successfully at a cost of only changing 4 bits.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

IV. RELATED WORKS

Existing systems are based on Asymmetric Algorithms such as RSA, DES, 3DES .AES is better than these algorithms shown in below figure 3[2, 3, and 8].

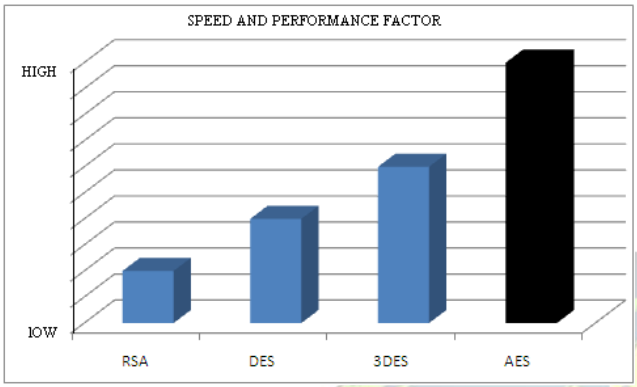


Fig. 3 AES Performance

V. PROPOSED WORK

In the proposed work a data security model is proposed to secure cloud data. This paper secures cloud by make sure of exclusive security requirements and tries to present a possible solution that eliminates the potential threats. The proposed system uses AES cipher that is used to ensure the confidentiality of involved data communications. The theoretical analysis shows the proposed schemes are provably safe and highly effectual.

A. AES Transformations

Cryptography technique is used to secure our data from the unauthorized access and the free movement over the web.

- Choosing pseudo random keyK. Convert each character to its respective ASCII code.
- Assigning all bytes in to a state which yields a matrix denotes M.
- Perform the AND operations on M and K yield the partial encrypted text for further operation.
- Four basic transformations are applied.

B. AES Encryption

In AES algorithm uses the following steps while encryption

- Get the key and select the secret message.
- Convert secret message into cipher message.
- Get the Cipher message and send to receiver as a secrete message.

C. Steganography Substitution

LSB Substitution is as follows:

- Getting the cipher message which is an unreadable form of message converted by using AES algorithm encryption technique.
- Taking a key image and using steganography LSB substitution technique to hide data in image.
- Generate encryption key, to read data from the image.

D. AES Decryption

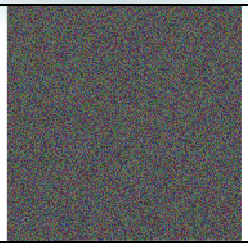
To get actual message we use data decryption method. The steps are:

- Get the cipher message and use the decryption key.
- original message will be obtained.

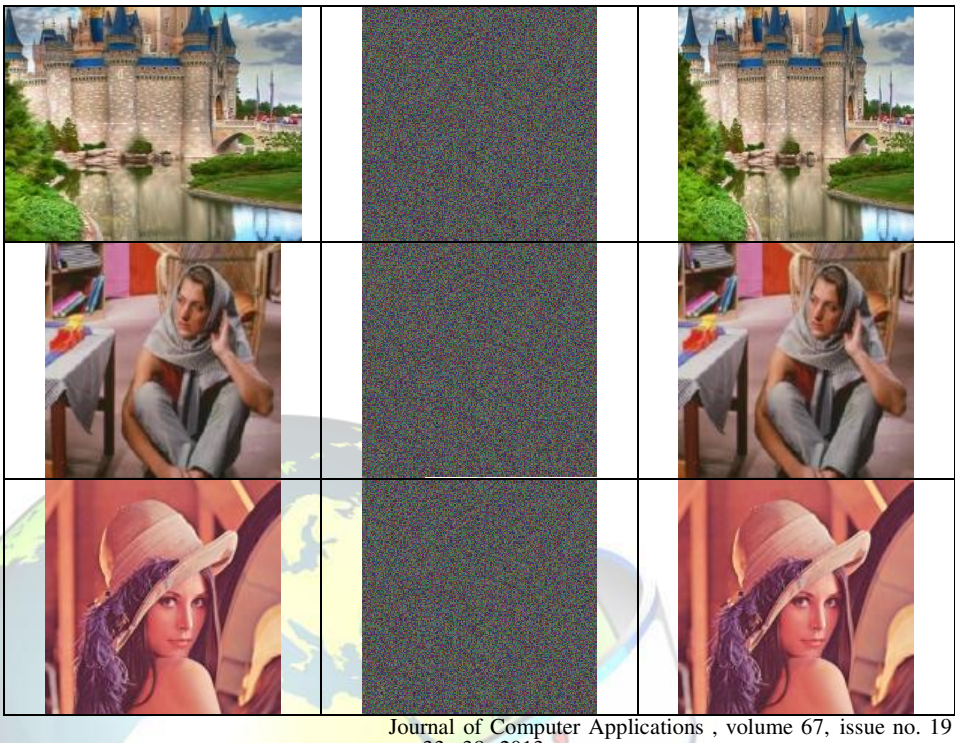
VI. EXPERIMENTAL RESULTS

After encryption the cipher text is saved as an image. This image is considered as a secret message as well as key image and embedded into cover image based on AES algorithm and Least Significant bit substitution and finally stego image will be produced, results are represented in the TableI below:

TABLE I
EXPERIMENTAL RESULTS OF THE PROPOSED METHOD

Key Image	AES Based Cipher Image	Stego Image
		

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016



VII. CONCLUSION

Cloud computing is a prominent technology offers various advantage to the user. It provides a virtual storage space to the user which could be used without bothering about the details of the entire mechanism. It offers a worthy number of paybacks for its users. However, it also nurtures some security plights which may slow down its fame. Vulnerabilities exist in cloud computing will be identified which helps the organizations to make the shift towards the cloud. The proposed work assesses the cloud security by using cryptography and steganography techniques together along with Improved Advanced Encryption Standard algorithm to secure data. The approach used in this work, will help to make a strong structure for security of data in cloud computing field or web. The future work of the proposed system will be extended by improving speed of the decryption process and also planned to reduce the size of the cover image using the compression technique.

REFERENCES

[1] Rachana, S. C., and H. S. Guruprasad. "Emerging Security Issues and Challenges in Cloud Computing." International Journal of Engineering Science and Innovative Technology, volume 3, issue no. 2 , pp. 485-490, 2014.

[2] Pant, Vinay Kumar, Jyoti Prakash, and Amit Asthana. "Three step data security model for cloud computing based on RSA and steganography." IEEE, Green Computing and Internet of Things (ICGCIoT), pp. 490 – 494, 2015.

[3] Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." International Journal of Computer Applications , volume 67, issue no. 19 , pp. 33– 38, 2013.

[4] So, Kuyoro. "Cloud computing security issues and challenges." International Journal of Computer Networks , volume 3, issue no. 5 , pp.247-255, 2011.

[5] Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." International Journal of Network Security & Its Applications , volume 6, issue no.1, pp.25-36, 2014.

[6] Joseph, Princymol, and S. Vishnukumar. "A study on steganographic techniques." IEEE Proceedings of Global Conference on Communication Technologies, pp.206-210, 2015.

[7] Christo Ananth, H. Anusuya Baby, "S-Box using AES Technique", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 3, March – 2014, pp 285-290.

[8] Padmavathi, B., and S. Ranjitha Kumari. "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique." International Journal of Science and Research (IJSR), volume 2, issue no.4 , pp. 2319-7064, 2013.

[9] Sarkar, Mrinal Kanti, and Trijit Chatterjee. "Enhancing Data Storage Security in Cloud Computing Through Steganography." International Journal on Network Security, volume 5, issue no.1, pp.13-19, 2014.

[10] Ryoo, Jungwoo, et al. "Cloud security auditing: challenges and emerging approaches." IEEE Security and Privacy, volume 12, issue no.6, pp.68-74, 2014.

[11] Roy, Ratnakirti, et al. "Evaluating image steganography techniques: Future research challenges." International Conference on. IEEE, Computing, Management and Telecommunications (ComManTel), pp. 309-314 , 2013.