Development of a Cloud-based Secure Text File Application using Hybrid Cryptography and Steganography

S.V.N.Srivalli, Ben SwarupMedikonda

Abstract; Cryptography and steganography are two popular ways to secretly send vital information. The first method distorts the message and the second method conceals the message's existence. In this paper we are using two phases to provide more security to the text files which are as follows. The first phase is the storing process where the users chooses a text file and split it into two equal parts, then encrypt both the subparts of the text files. One with the Blowfish and the other with the AES algorithms then merge both the encrypted parts of the text fileand uploaded into the ownCloud. Then the keys that are used to encrypt both the subfiles are hidden behind a cover image by using the steganography LSB technique and sent to the user mails. The second phases are the retrieval process where theuser retrieves the keys from the stegno image and decrypts both the subparts of the text files and merge both the subparts. Thus, in this way we are providing more security to the text files that are uploaded into the cloud.

Keywords; AES, Blowfish, Cryptography,Frequency domain, LSB, Spatial domain, Steganography.

I. INTRODUCTION

Cloud computing is another new improvement in the field of computer science and networking. It depends on the guideline of virtualization, which implies that there is a single machine and different clients are sharing this machine.It has three levels of services that are like this their own resources.(i)Infrastructure as a service (IaaS)(ii)Platform as a service (PaaS)(iii)Software as a service (SaaS).In the IaaS the hardware assets, for example, hard-disk, memory, networking resources are given in the rent and are charged according to the usage. In the PaaS, this not only provides all the facilities as in IaaS, yet additionally gives operating system facilities, their updates, etc.Consequently, make all work effectively. At long last, the SaaS, which is the most flexible and easy to utilize. Each layer of cloud computing is associated with various layers of cloud infrastructure, i.e. (i) Application Level (ii) Network Level (iii) Data Storage Level (iv) Virtualization Level (v) Authentication and Access Control Level. It has all the highlights of IaaS and PaaS and gives the opportunity of freedom to choose software applications from a bundle of already available resources. Although cloud computing gives ondemand services to its clients and it is very useful in today's life, but it has some of its own set of cons of different layers. In the data storage level, which includes various challenges such as (i) Data Location (ii) The concern of data security (iii) Who has right to see their data? The goal is to provide security for the uploaded data in the cloud by using Hybrid cryptography and Steganography methods and techniques.

Hybrid cryptography is a is a protocol using multiple ciphers of various types together, each of its best benefits. One common approach is to create an irregular secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key. The message itself is then encoded by using the symmetric figure and the secret key. Both the encoded secret key and the encrypted message are sent to the recipient. The recipient decodes the secret key first, by utilizing their own private key, and after that utilizes the key to decode the message.Steganography is a data hidden within the data. It is an encryption technique that can be used along with the encryption as an extra secure method in which to protect the data. These techniques can be applied to the images, videos or an audio file. The main objective of our proposed system is to provide the security to the text file that which is going to be uploaded into the cloud. we are using the hybrid cryptography algorithms such as AES and Blowfish which are going to be used for encrypting and decrypting the text file. At which the file, i.e.; needed to be uploaded into the cloud is divided into the two parts and each part is encrypted by using the above mentioned two algorithms. Now, the keys that are being used to encrypt the sub parts of the text file is hidden behind the image with the help of some steganography methods such as follows.

(1) Substitution Methods
(2) Transform Domain Techniques
(3) Cover Generation Methods

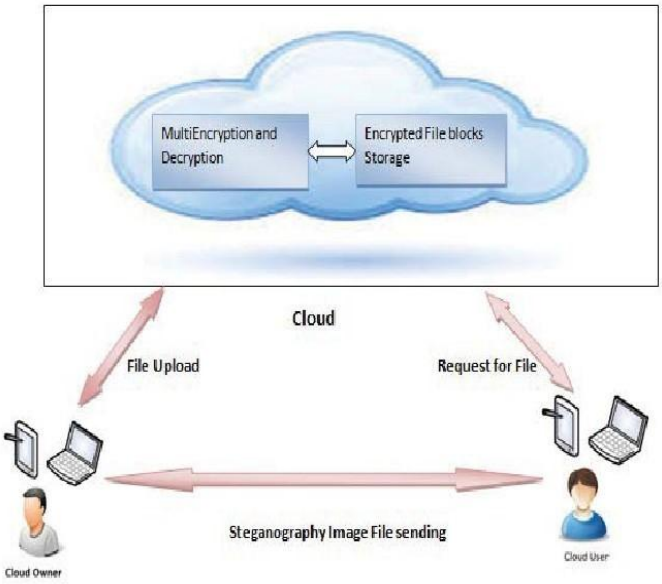
This paper is organized as follows: Section 2 describes the recent research on cloud-based security techniques. Section 3 explains about the proposed system in our project. Section 4 describes the methodology used in the proposed system. Section 5 describes the results. Section 6 concludes the paper.

II. LITERATURE SURVEY

In the paper "Review paper on Enhancing Data Security for Cloud Environment Cryptography and Steganography Technique" by Deepika and GurjeetKaur [2016]the key conclusionis that, a technology called Safe and secure technique in the Cloud technology Environment has been prop osed to provide privacy without any loss of information. This maintains sensitive data regarding the individual being preserved. As the randomized index value of this technique is equivalent to pixel values of the picking image transmitted into the cloud, instead of the real data. very difficult and its hard and it's hard to restore actual data

without recognizing what those bits and bytes point to. This paper "A Hybrid Technique for Enhancing Data Security". G.Manikandan, P. Harini, K. Harini Rajalakshmi [2018]restores a modern method for data security improvement. The machine's novelty is that the original plain text is partitioned into many other chunks and each chunk will be diaturbed, exchanged and shifted in the same sequence. In the encryption algorithm, the modified simple text is inserted as a direct input. AES or encrypted and decrypted algorithms are used. The crypted cipher text will be placed in the decryption algorithm to obtain the modified plain text. In this paper "Proposed System for data hiding using Cryptography and Steganography". Dipti Kapoor Sarmah1, ehaBajpaihasproduces a new cryptography and steganography

Fig. 1: Architecture of the Proposed System



integration system using four keys that could prove to be in future a very safe data communication technology. Steganography is a powerful tool that allows people to connect, even to achieve in the first place, without eavesdroppers, especially in combination with cryptography. We are even aware that a form of communication exists in the first place. The method proposed offers an acceptable quality of the image with very little image distortion. This Crypto / Stegno system's main advantage is that the method used for crypting, AES, is very safe and DCT steganography technology can hardly be identified. This paper"Multi-level Security: Data Sharing using Cryptography and Steganography in Cloud Computing". Deepika. J, Bharathi Dasan. V. S, Vidhya. K" [2014]considered the fore mentioned drawbacks and decided to compress the key requirements. So, a new approach called steganography technique is used along with the KAC approach to provide multiple layer of security for data owner who upload the data and data user who download the data. There is more preserving data integrity and confidentiality. So,that it is a challenging problem for a breaker/interrupter to inject or to remove data from an original content and it's a toughest work for other parties to predict the original data from a cipher format of the original one, because of the introduction of the multiple time encryption (Cascade Encryption). In this paper "Data Security in Cloud Computing using Encryption and Steganography".Karun Handa, Uma Singh [2015]indeed, cloud computing can be a boon in today's workplace environment, so this paper tries to address cloud computing - key data security issues so that data centers can provide a good environment for data protection. This scheme addresses the question of security of data and provides a high level of security by using client encryption and server steganography on the side.On the server side, a highly secure model isprovided that not only fixes the issue of data protection, but also makes it much easier to implement and use. This paper *"Hybrid Approach to Text & Image Steganography using AES and LSB Technique".* Vikas M, Yashwanth E, VeereshSanath Krishna S, Narender .M [2018]explains the method in this paper will help us to reduce risk of security while transferring secret information over the network. The proposed system is user friendly and anyone with basic computer knowledge can use the system without any difficulties. Further, the system can be extended to different types of files like Audio, Video, etc. also it can be applied to different formats of files.

III. PROPOSED SYSTEM

The main objective of our proposed system is to provide the security to the text file that which is going to be uploaded into the cloud server. Firstly, the user selects a text file and then this text file is splitted into two equal parts. Then the both splitted text files are encrypted with the Blowfish and AES algorithms i.e. one text file with the Blowfish and the other text file with the AES.Now, both the encrypted subparts of the splitted text file are uploaded into the ownCloud server and the keys that are being used to encrypt both the subparts of the splitted text filesare hidden behind a cover image with the help of the LSB (Least Significant Bit) steganography method. The following figure is the architecture of the proposed system which consists of six components in it which are as follows.

The following are the six components that are used in the architecture of the proposed system.

(i) **Cloud Owner:** The cloud owner chooses the text file and split it into two sub files, then encrypts both the sub files with the Blowfish and AES algorithms.

(ii) **File Upload:** The cloud owner after encrypting the text file uploads the file into the cloud.

(iii) **Cloud:** It is used to store huge amount of the data which can be accessed at anywhere and at any time whenever the user requires.

(iv) **Steganography Image File Sending:** The cloud owner after encrypting the files with a key, this key is hidden behind the image by using the steganography LSB technique and it is sent to the cloud user through their mails.

(v) **Cloud User:**This cloud user is an authorized user who can access the files stored in the cloud who can access the files anywhere.

(vi) **Request for the File:** The cloud user requests the cloud owner to access the files that are stored in the cloud.

IV. METHODOLOGY

To provide more security to the files uploading into the cloud in our project we used the following two phases.

(i) **Storing Process**

(a) To choose a text file.
(b) Split the text file into two equal sub files.
(c) Encrypt the first sub file with the Blowfish algorithm.
(d) Encrypt the second sub file with the AES algorithm.
(e) Uploads both the encrypted sub parts of the text file into ownCloud.
(f) To hide the keys used to encrypt the files behind an image by using the steganography LSB technique.

The sequence of steps for the storing process is shown in the following figure 2.

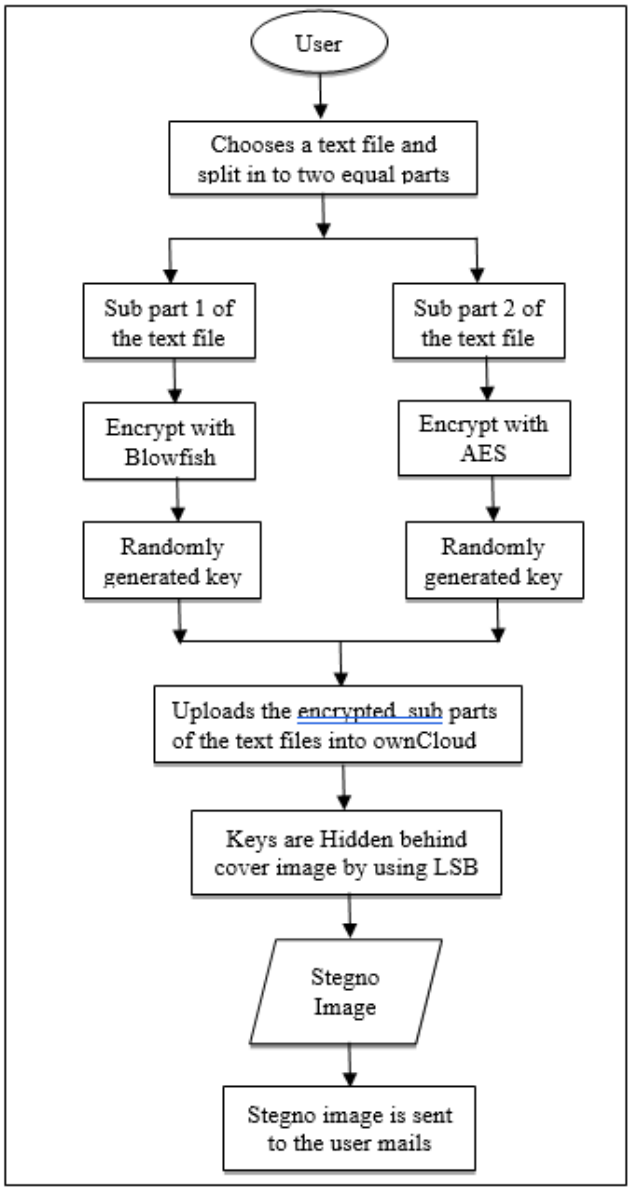


Fig. 2: Sequence of steps for storing process

(ii) **Retrieval Process**

(a) Retrieve the keys hidden behind the image.
(b) Choose the files in the ownCloud which the user needs.
(c) Decrypt the first sub file with the Blowfish algorithm.
(d) Decrypt the second sub file with the AES algorithm.
(e) Merge both the files into as one file.

Thus, the above two phases will provide more security to the text files that are uploaded into the cloud. The sequence of steps for the retrieval process is shown in the following figure 3.

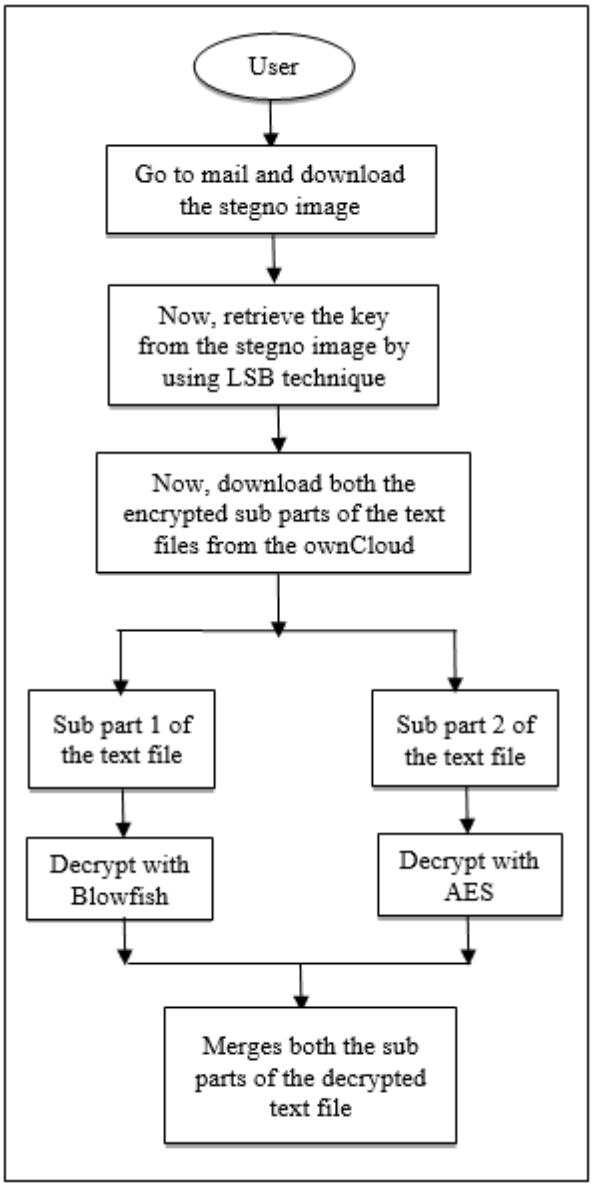


Fig. 3: Sequence of steps for retrieval process

Thus, the above two figures i.e. figure 2 and figure 3 are the

sequential steps in the storing process and the retrieval process in which the user needs to perform to which will reduce the risk of the security while transferring the text files. At first the user performs the storing process and next the user performs the retrieval process.

V. RESULTS

The below figures are the screenshots of the proposed system.

Fig.4: Login page

Firstly, the user gets login with an authorized username and password.

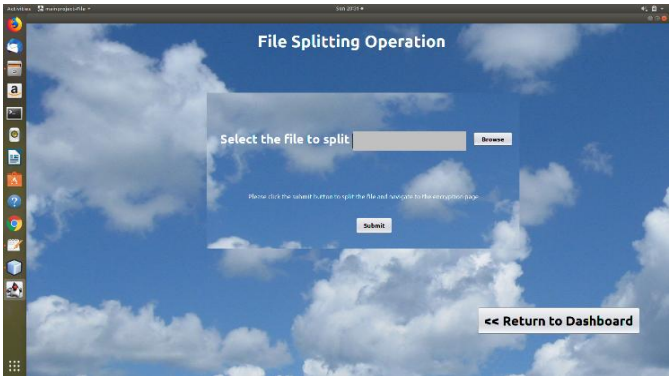


Fig.5: File splitting page

In the figure 5 the user selects the text file which needed to be split and split the text file into two subparts.

Fig.6: Encryption with Blowfish

In the figure6 the user chooses the subpart 1 of the split text file and encrypt with the Blowfish algorithm with a randomly generated key.

Fig.7: Encryption with AES

In the figure 7the user chooses the subpart 2 of the split text file and encrypt with the AES algorithm with a randomly generated key.

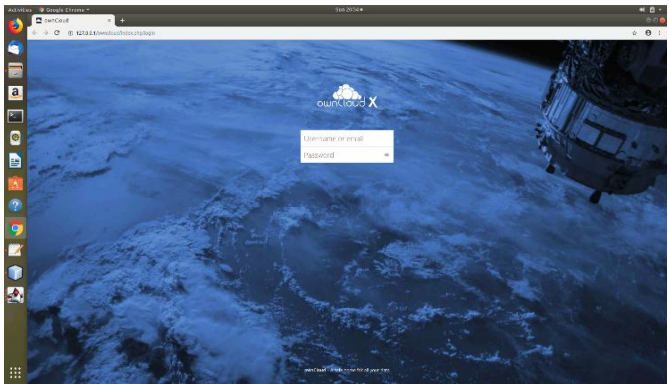


Fig. 8: ownCloud page

In the figure 8 the user uploads both the encrypted sub parts of a split text file into the ownCloud server.

Fig.9: Data Hiding page

In the figure 9 the keys that are randomly generated while encrypting both the subparts of a text file are hidden behind the cover image by using the LSB steganography technique and sent to the respective user mails.

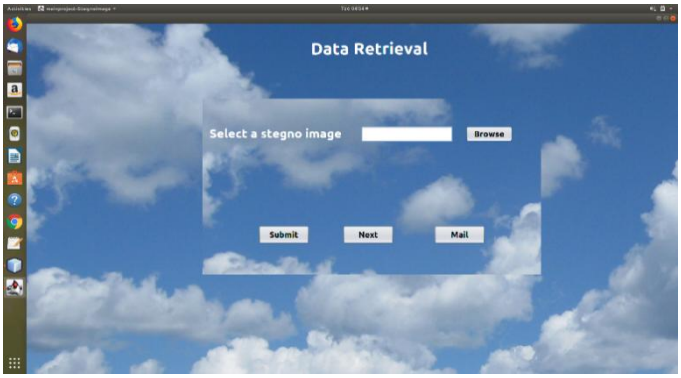


Fig. 10: Data Retrieval page

In the figure 10 the user retrieves the keys from the stegno image whenever the user needs to decrypt the encrypted files.

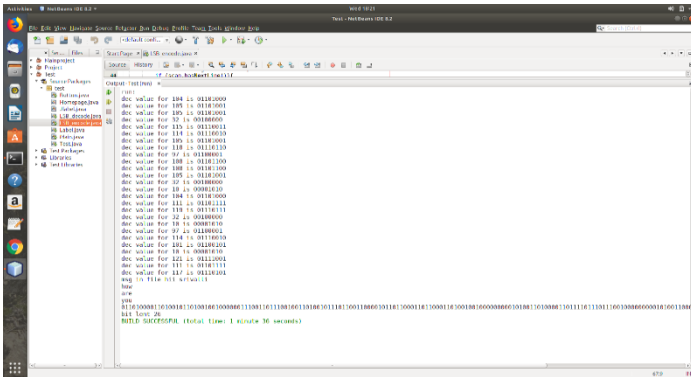


Fig. 11: Output for the data hiding

The figure 11 is the output screen for the data hiding behind the cover image by using the LSB steganography technique.

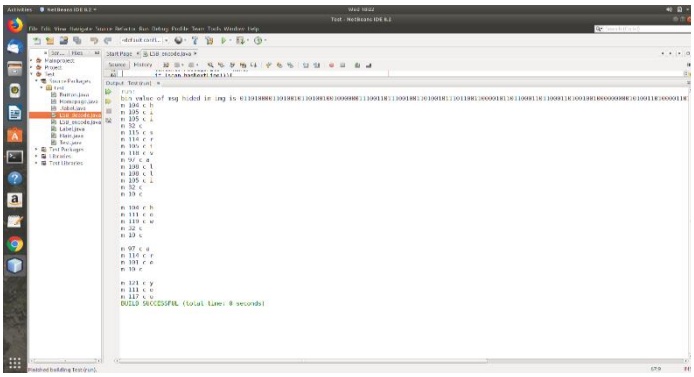


Fig. 12: Data Retrieval page

The figure 12 is the output screen for the data retrievalfrom the stegno image by using the LSB steganography technique. Now, the user decrypts both the encrypted sub parts of text file and merges them into as one text file.

VI. CONCLUSION

This paper introduces a modern approach which will help the user to reduce risk of security while to the text files.TheProposed system is user friendly and anyone with basic computer knowledge can use the system without any difficulties. The novelty of the system is that the original text file is divided into two equal subparts and each sub part will undergo encryption by using Blowfish and AES and then these subparts will be merged and uploaded into the ownCloud server and the keys that are used to encrypt the sub parts of the text file are hidden behind the cover image by using the LSB steganography method and then the stegno image is sent to the respective user mails. The results for this proposed system are mentioned in the above results section with the output screens as well.

REFERENCES

1. "Review paper on Enhancing Data Security for Cloud Environment Cryptography and Steganography Technique" by Deepika and GurjeetKaur [2016].
2. "A Hybrid Technique for Enhancing Data Security" by Manikandan .G, Harini .P, K. HariniRajalakshmi [2018].
3. "Proposed System for data hiding using Cryptography and Steganography" by Dipti Kapoor Sarmah1, Neha Bajpai.
4. "Multi-level Security: Data Sharing using Cryptography and Steganography in Cloud Computing" by Deepika. J, Bharathi Dasan. V. S, Vidhya. K" [2014].
5. "Data Security in Cloud Computing using Encryption and Steganography" by Karun Handa, Uma Singh [2015].
6. "Hybrid Approach to Text & Image Steganography using AES and LSB Technique" by Vikas M, Yashwanth E, Veeresh, Sanath Krishna S, Narender .M [2018].
7. "An Information Security Technique Using DES-RSA Hybrid and LSB" by Sandeep Singh, Aman Singh [2014].
8. "An introduction to steganography methods" by Masoud Nosrati, Ronak Karimi, Mehdi Hariri [2011].
9. "Security Issues for cloud computing" by Kevin Hamlen, Murat Kantarcioglu,Latifur Khan, Bhavani Thuraisingham [2010].
10. "An Overview and Study of Security Issues & Challenges in Cloud Computing" by Rajesh Piplode Umesh Kumar Singh [2012].
11. "Secure File Storage in Cloud Computing using Hybrid Cryptography Algorithm" by Bindu Bala, Lovejeet Kamboj, Pawan Luthra [2015-19].
12. "Hybrid Cryptosystem for Secure Data Storage" by Mihir Shah, Prof. Sujata Pathak [2017].

AUTHORS PROFILE

Ms. S.V.N. Srivalli received B.Tech (CSE) from Vignan's Institute of Engineering for Women, Visakhapatnam, India. Currently, Ms. S.V.N. Srivalli is pursuing her M.Tech (CSE) at Vignan's Institute of Information Technology, Visakhapatnam-530049. Her research areas include cloud computing.

Dr. Ben Swarup Medikondareceived his B.Tech, M.Tech and Ph.D from N.I.T Warangal, university of Hyderabad and Andhra University Visakhapatnam respectively. He is presently working as Professor and Dean of Academics in department of Computer Science and Engineering at Vignan's Institute of Information Technology Visakhapatnam. His primary research areas are advanced software engineering, safety critical software systems, cloud computing and internet of things.