Cloud Computing Security Using Steganography

Santosh Kumar Singh[1], Dr. P.K.Manjhi[2], Dr. R.K.Tiwari[3]

Research Scholar, Department of Computer Applications, Vinoba Bhave University, Hazaribag, India [1]

Assistant Professor, University Department of mathematics, Vinoba Bhave University, Hazaribag, India [2]

Professor, H.O.D CSE, R.V.S College of Engg. & Tech., Jamshedpur, India [3]

ABSTRACT

Cloud computing provides the ability to use computing and storage resources on a rented basis and reduce the investments in an organization's computing infrastructure. With huge benefits cloud computing also brings with it concerns about the security and privacy of information. Now a days cloud computing is used by smart mobile applications so there are some security and privacy concerns on data provided by the cloud providers. In this paper, we demonstrate how Steganography, which is a secrecy method to conceal information, can be used to enhance the security and privacy of data maintained on the cloud by mobile applications. Our proposed design works with a key, which is securely surrounded in the image along with the data, to provide an additional layer of security.

Keywords: Cloud computing, Mobile Computing, Data Hiding, Steganography, Encryption

1. Introduction

Cloud computing is a recent development in information technology that moves computing and data away from desktop and portable PCs into large data centre. Cloud refers to applications delivered as services over the internet as well as to the actual cloud infrastructure namely, the hardware and systems software in data centers that provide these services [1].

In [2], a combined approach of steganography with LSB encoding technique and Data Encryption Standard algorithm (DES). In which they encrypted data by DES encryption algorithm and then embedded the decrypted data by the LSB method. As LSB is not much secure enough, we can say that this system doesn't provide better security. An advanced technique to share and protect cloud data using multilayer steganography and cryptography is used in [3]. Where data is encrypted by the AES (Advanced Encryption Standard) algorithm, and then encrypted data embedded in a cover image by using Hash-LSB algorithm.

In mobile cloud computing, our data are stored on device or cloud. As we know day by day the mobile with internet facility continue growing, Internet based several security threat is going to be serious issue. In this paper, we are trying to discuss the working concepts of mobile cloud and its number of security issues. In this paper, we are trying to focus on security of mobile cloud computing using mobile devices. Steganography has been used to hide messages inside some kinds of contents like video, audio and image in such a way that it does not allow someone or anyone to detect or access that there is a secret message present. Basically Steganography is used on text, audio, video and image

2. Steganography

The Steganography imply concealing data or information, it allowing data/information to be transferred to the receiver end without knowing that the original message still existed. The processes generally imply placing a hidden message within some transport medium. Steganography is fully different from cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages which transforms a message into a non understandable string that can only be deciphered by the recipient end. As in cryptography, it is normal that a data/information in the form of message has been sent, but the data/information of the message is interchanged. As in steganography, the casual observer has no idea about that a data/information in the form of message had been sent.

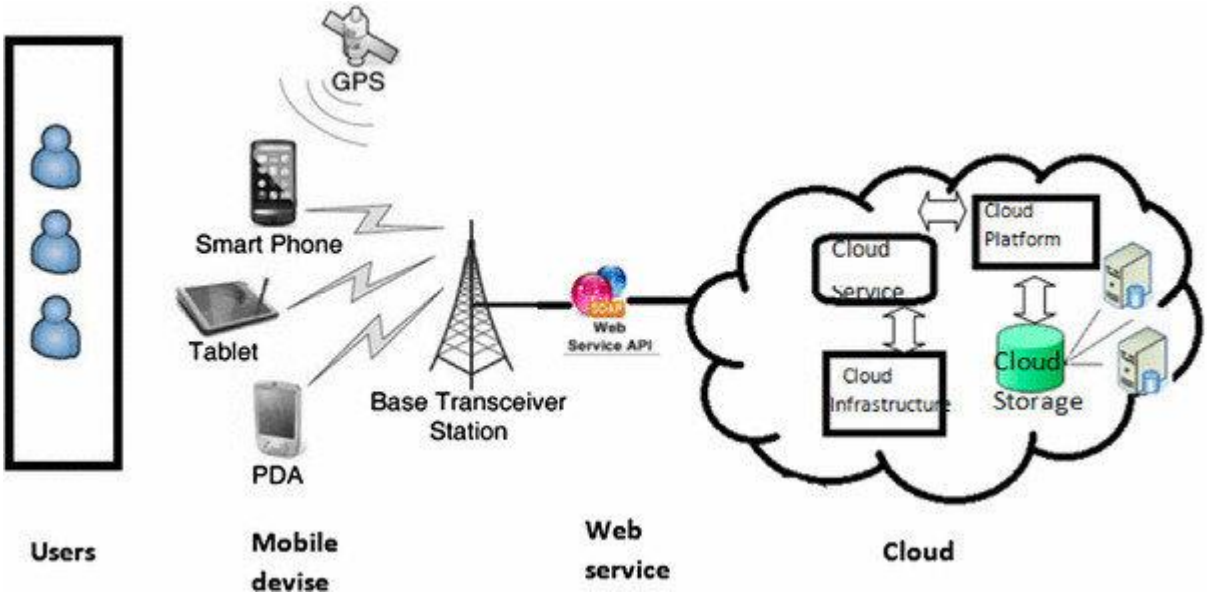

Figure1. Mobile cloud computing

Figure 1 showing the architecture of Mobile Cloud Computing. In **Figure 1**, the main parts or components of the Mobile Cloud Computing architecture are mobile user with internet connection, smart mobile device and cloud service provider which is the essential part of architecture [5].

Figure 2 represents the steganography architecture. This model consists of the following components:

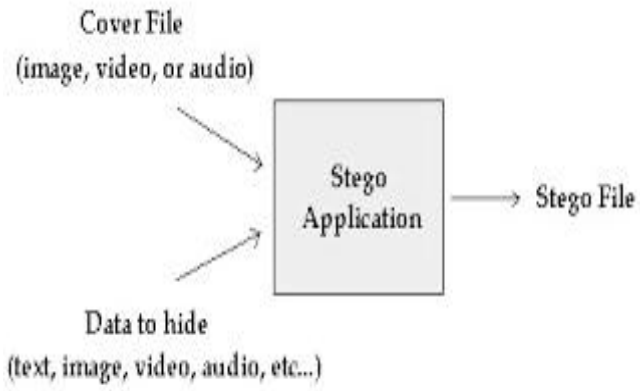

Figure2. The architecture of Steganography

Stego Application will take as an input of Cover file and Data to hide and produce after process as a stego file. First input is cover file which may be in the form of image, video or audio and second input is data to hide which may include in the form of text, image, video, audio, etc, after inputting the inputs into stego application it will process the data and produce stego file which will be secure and safe.

Type of Steganography can be: (1) Steganography (pure), (2) Steganography (symmetric) and (3) steganography (asymmetric) [6]. Steganography (Pure) - any of information no need to exchange. Steganography (Symmetric) - exchange of keys does not require prior to sending the messages.
Steganography (Asymmetric) - exchanging keys does not require prior to sending the messages.

Methods of Steganography

Generally most common approaches for information hiding are: (1) Least Significant Bit (LSB) insertion, (2) Masking and filtering techniques, (3) Algorithms and Transformation [4].

Least Significant Bit- Most common and widely used methods of steganography useful alternation to the least significant bits (LSB) of each colour pixel within a digital image. A digital image like bitmap (BMP) or a graphic interchange format (GIF) contains thousands/ millions, of pixels, or colored dots, to create the picture. “Each pixel on a computer monitor selects from three primary colour variations: red, blue and green, also referred to as RBG”. In a 24-bit image, each of these three colours is represented by one byte, or eight bits, with a bit being the smallest unit of data that can be stored on a computer. Each bit within the byte is assigned a value so that the sum of the bits totals anywhere between 0 and 255. The bits are valued from right to left – 1, 2, 4, 8, 16, 32, 64 and 128. For example, the colour black would be represented as

00000000, 00000000, and 00000000. The colour white would be represented as 11111111, 11111111, and 11111111. Changes to these bits are reflected as a change in colour and light quality within the image.

In its most general form, the LSB method of steganography involves changing the lowest valued bit in each byte. This is the byte of far right-hand bit, which is represented having a value of one. Changes to this value will change the colour displayed in the image, but the change is very small that it is not visible by the normal human eye. Since text characters or string are represented as one byte, or eight bits, for each letter, steganography software, such as S-Tools, can replace one bit from a byte of text for the LSB of every colour byte. This process is continued until the whole file to be concealed has been embedded into the carrier file.
Basically steganography applications with the LSB method of substitution randomly take which bits will be used for the process in steganography. More developed applications first evaluate the carrier image and set the boundaries which bits should be altered to minimize detection and maintain the original aspect of the image [7].
Masking and filtering technology works according to watermarking hide the information by marking the image as in paper watermarking. Said technology may be used on 24 bit gray scale or colored images. Watermarking techniques are much suitable into the image no tension for image lost or unstructured form, they may be applied without any tension of image destruction. The normal human visual system cannot detect or identify changes in JPEG images. The algorithms and transformation technique basically compress the size of image which uses mathematical functions to conceal the least bit coefficients in the compression algorithms for reducing the size of images.

3. Proposed Approach to Secure Data from Cloud Provider

Basically we are working on the data to be secure on cloud under the control of cloud manager of our data which we have uploaded on trust basis. The suggested solution allows a user to secure his own data maintained by cloud provider in the cloud environment. In this current era mobile phone is the heart and soul for the development of each and everyone. But some issues over there like data protection, processing capability low, energy supply, and storage capacity.

Software working model of the proposed system with the steganography application (SA) shown in **Figure 3**. The main component of our model include the following components like-

User- the role of user is to select an image and combination of key and data. Smart Mobile device- able to run steganography application
Steganography application – used to encapsulate data and the key in the image provided by the user.
Stego image- Steganography application produce stego image which we send to cloud. After that software retrieves data from the image if user's entered key matched.

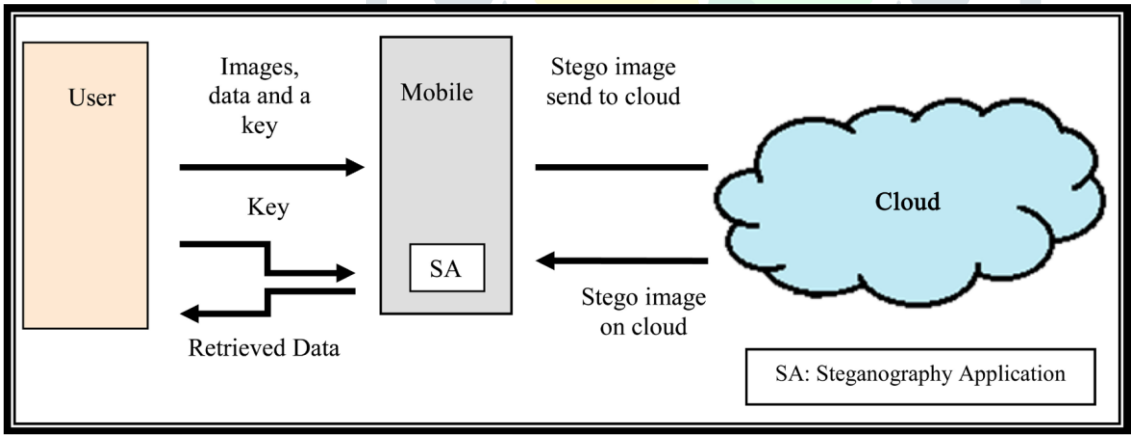

Figure3. Proposed system

The proposed system is the combination of cloud computing and steganography. In this model, user will select an image, after that enter the data and the keys as the input now this input will be used by the steganography application, which is installed on the user's mobile device. The steganography application converts the inputs and produce stego image to be accumulated on the cloud. As we know internet connection is must for cloud access. When used want to access the data which is on the cloud he has to use steganography application and he has to input the key if key matched then user easily and safely access the data.

In this paper we have used the least significant bit technique to hide information, which makes the mobile cloud computing application robust, dynamic and least concerned for image misrepresentation. Further we will use 24 bit images which makes possible of 16,000k different combinations that can easily conceal data in a way that it will be quite tough to detect any difference between the modified image and the original image or actual image.

If we want to provide more security, algorithms based on encryption are used but it will increase the load on the processor so that processor will be slow which affect the performance. To overcome this problem we have used the concept of a key. Now key is encapsulated into an image combined with the actual data or information, with the help of algorithm calculating

bytes of location where the key has been reside. Simply user will install this software and only remember the key for successful and secure communication.

4. Implementation

Basically mobile phone is much easier to access our online accounts and user prefers mobile applications for their work. So he has number of accounts their login id and passwords and there is a chance to forget these login id and passwords, in such situation user can store limited amount of information or data on cloud, by mobile using steganography, which will secure user data from cloud administrator. If user or customer is storing their information on cloud then they can easily access data from any location without any tension of losing important data.

This application is suitable for low amounts of data with less processing power and low battery usage. Therefore it increases the performance of the overall application and the mobile device. This approach combines and improves the trust in mobile computing as well as improves the efficiency of cloud computing, so that user can use mobile applications with more secure way without any tension of data damage.

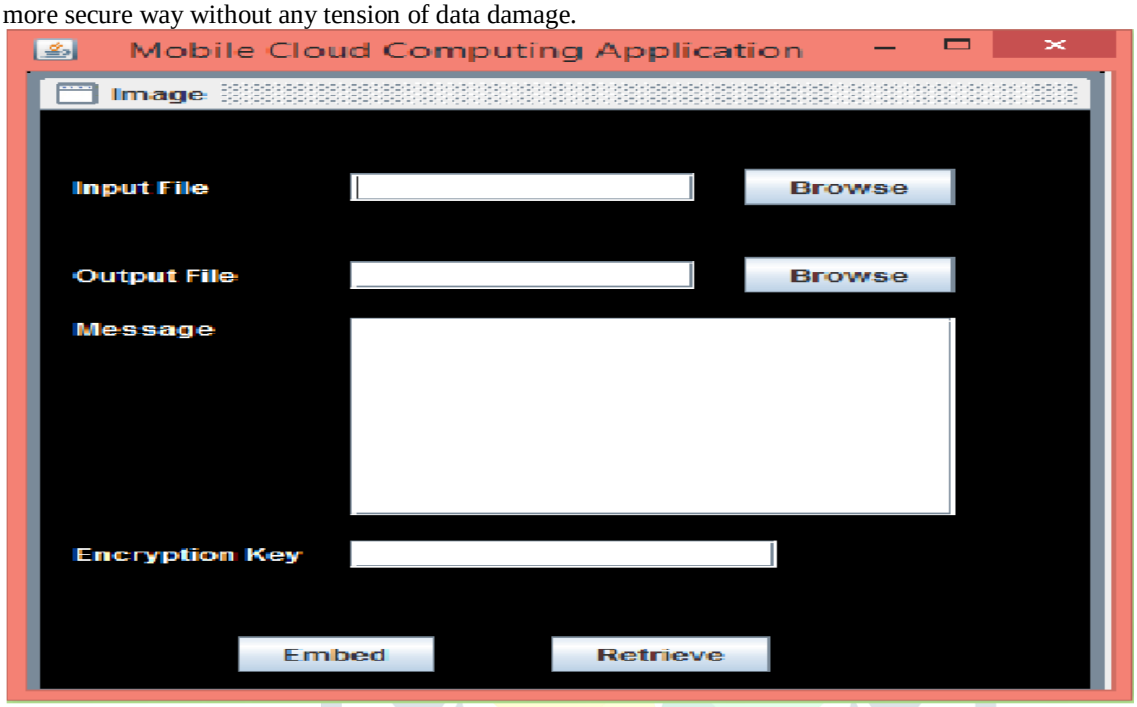

Figure4. Home page

Above **Figure4** shows the Mobile Cloud Computing Application's home page, there is a facility to choose input and output image path it depends upon the user where user can select an input and output image path, and enter data and a key encapsulated into an image.

Below **Figure 5** is the original image as an input on which software works and converts it into stego image and **Figure 6** is the stego image which is the converted form of original image created after encapsulated secret message and the key. Image is little changed but it cannot be identify by normal human eyes.

Figure5. Original Image

Figure6. Stego Image

5. Conclusion and Future Work

In this paper proposed steganography application can be used for data security without others involvement. The proposed system will work efficiently with the key, but if he/she loses the key, then the system does not have any provision to recover the key, so in this case a user might cause lose the data. This is the serious drawback on which we will work in future. Proposed system is only applicable for limited data so in future we will try large data processing. In the future we can say, cloud and proposed model will work together in efficient manner.

References

1. Singh, S. K., Manjhi, P.K., Tiwari, R.K., and Vadi, V. 2018, A Secure Communication Scheme for Cloud Environment. International Journal of Computer Engineering and Applications, vol. 12, issue 4, pp. 97-106.
2. Karthikeyan, B., Deepak, A. K., S., Subalakshmi, A., and Vaithiyanathan, V. 2017, A combined approach of steganography with LSB encoding technique and DES algorithm", Proc. of 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and BioInformatics.
3. Ranjan, A. and Bhonsle, M. 2016, Advanced technics to shared & protect cloud data using multilayer steganography and cryptography", Proc. of IEEE International Conference on Automatic Control and Dynamic Optimization Techniques.
4. Kumar, A. and Pooja, K. 2010, Steganography: A Data Hiding Technique. International Journal of Computer Applications, 975-8887. http://dx.doi.org/10.5120/1398-1887
5. Shamim, S., Sarker, A. and Bahar, A. 2015, A Review on Mobile Cloud Computing. International Journal of Computer Applications, **113**, 4-9. http://dx.doi.org/10.5120/19908-1883
6. Mahajan, S. and Singh, A. 2012, A Review of Methods and Approach for Secure Steganography. International Journal of Advanced Research in Computer Science and Software Engineering, **2**, 484-488.
7. https://cyber-defense.sans.org/resources/papers/gsec/steganography-corporate-environment-106511
8. Hanen Jemal, Kechaou Zied and A. B. Mounir . 19th july 2016, An enhanced healthcare in mobile cloud computing environment, Springerlink.com, DOI 10.1007/s40595-016-0076-y.