ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)

International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)

Cochin College of Engineering & Technology

Vol. 4, Special Issue 1, June 2015

Audio Steganography Scheme to Advance the Security of Data in Hybrid Cloud

Hasna Parveen O H

Department of Computer Science and Engineering, Cochin College of Engineering and Technology, Kerala, India

Abstract: Steganography is the art of science dealing with the hiding of secret data inside an image, audio, video or text files. One of the foremost differences between the steganography and cryptography is that even as we using cryptography technique we can't spot the original data but we discern that data are hiding as encrypted format. But despite the fact that we are using steganography we can't sense the charisma of secret data. Hence it is healthier to use steganographic approach to hide data in hybrid cloud to guarantee the security. In our paper it is about how to develop the security of data in the hybrid cloud. A hybrid cloud consists in cooperation of public and private data. Here the public data can be honestly accessed by the normal users devoid of any corroboration. But in the turn of a private data, it is obscured using an audio file. This private data can only evident to the owner and the personage whom the owner wishes to share the data. Hybrid cloud furthermore consist a section called OTP generator which engender one time password. While the owner tries to retrieve the data then a password is send to him. After the verification he can disengage the secret data in a private browser. So when hackers try to attack the cloud or private data he will be able to see simply the audio file. He can't be aware of the presence of data. This approach is mainly based on the property of HAS.

Index Terms: Steganography, OTP generator, Hybrid cloud, HAS.

INTRODUCTION

Secure distribution of data and data transmission over the internet is a vision from the time when the manifestation of internet. Hybrid clouds such as Amazon web services consist of both private and public data. In that some of them are extremely sensitive and some other are medium sensitive and some of them can right to use without any restriction.

Today we are generally used cryptographic approaches for secure data storage and sharing. But whatever we do to secure our data day by day attacker turn out to be more and more intelligent and they perform new methods to crack the data.

While we using the steganography it conceal the existence of message. And also it doesn't alter the structure of message, but hide it inside a cover image, text or audio. We mainly go for audio steganography is because audio can hold more data than an image since audio is large than image. And also a slight deviation in amplitude can store up a gigantic amount of data.

What Is A Hybrid Cloud

The hybrid cloud such as Amazon web services, Google cloud are the blended with public cloud and private cloud [1]. The main advantage of hybrid cloud over the public cloud is that it can trim down the access time and latency. Due to the less storage cost many of the organizations use this hybrid cloud to store their data. But the major risk behind this is a single point of failure may cause the entire process of all organization.

These technologies are mainly used in health care industry, used by Law firms, in retail sales etc against the lost, theft, or any natural hazards that may leads to the missing of original document or evidence.

Audio steganography

A perfect audio Steganographic technique aim at embedding data inside a cover audio in an unrevealed, vigorous and secure way that can only extracting it by authorized people. Hence, up to this era the main challenge faced in the audio steganography area is how to obtain robust and efficient steganographic systems [3].Unlike cryptography steganography doesn't reveal the presence of data. Audio steganography is based on the masking effect of Human auditory system (HAS). This means that the week sounds are undetectable in the presence of large sound [2]

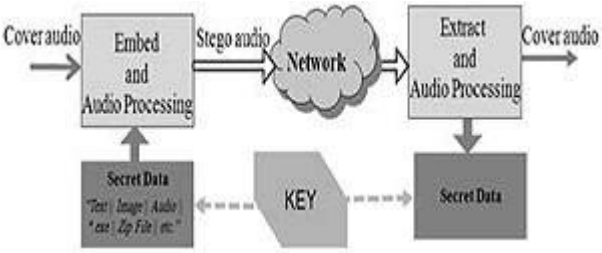
Cover audio
Embed and Audio Processing
Stego audio
Network
Extract and Audio Processing
Cover audio
Secret Data
"Text | Image | Audio | *exe | Zip File | etc."
KEY
Secret Data

Fig: Audio steganography technique

RELATED WORKS

Recently now we are using the steganographic approach in hybrid clouds. Mostly we are using the embedding information in LSB, pseudo random embedding .But these techniques are not much efficient due to limitation of computational resources and they use too much time [5].

The major risk faced by the hybrid cloud is data leakage, storage and protection of the sensitive data. Bo Liu, Erci Xu, Jin Wang and their team implement a new method to defense the audio steganographic attack in the cloud storage system [6]. For that they implement an enhanced RS Algorithm and SADI Algorithm. RS Algorithm are used to find the steganographied audio file. SADI Algorithm which is used to interfere all possible places in the suspicious file. But here in case of steganographied file the change in the hiding place may destroy the information. At the same time innocent files also get distorted due to the interference. But if the distortion is in the LS place the slight change in the sound doesn't recognized easily.

According to Xueli Huang and Xiaojiang Du they proposed a new approach for data privacy in hybrid cloud [7]. Here the image data which holds the sensitive are divide into n number of blocks. After that we apply random noise into the blocks. Then shuffle these blocks randomly. Thus we obtain an unreadable image. This image is send to the public cloud and the information about random shuffle and noise are stored inside a private cloud. This approach can reduce the storage overhead in private cloud. But the major drawback of this approach is that the shuffled image can give hacker a clue about the image contains some sensitive information. And also we want to consider the unauthorized public cloud providers

Aishwarya KauJ, Sheoli Tu, and Rachna Jain in their paper a combined encryption stego-object processing is about the cloud storage security [8]. Here they encrypt both the key and message. The key is encrypted with Shamir's Algorithm and the message is encrypted by Two fish algorithm. Due to this dual encryption the leakage of secure data is impossible. Here the message is hidden inside image and they use audio processing for sending the secret key. Even though this is a good approach if the TPA is not a trusted one or the malicious system admins can capture this key. Along with that while we transmitting through the network some time the crackers also try to capture the key. Because whatever precautions we do against attacker day by day attackers also come with new ideas in hacking.

There are many audio steganographic approaches for the secret sharing of information [3][5].They are different in their hiding domain. Mainly they are temporal domain, frequency domain, wavelet domain. Then I go through a comparative study among these techniques. I realize that if the technique is highly robust then it have less embedding rate. But if the systems have high embedding rate then it has less recovering quality and less security.

Proposed Approach

The steganography technique is pertaining while we covet to conceal the information. There are various reasons to hide information from the community; this can be done to thwart the unauthorized personality from the attentiveness about the occurrence of undisclosed records. They may be of trade secrets, may be significant chemical formulas or sometime it may be copyright information.[4]

This paper mainly concentrates on how an audio steganography can be applied to the hybrid cloud to improve the storage security. This approach allows the proprietor to embed the secret message within the cover audio without affecting the superiority of the original audio. Different file format like MP3, WAV, AU audio files can be preferred as the cover audio. Our target users are owners of organization who use hybrid cloud like Amazon Web Services or Microsoft Azure to store their business information.

Here in our approach we have a hybrid cloud which consists of public and private information. A few of the informations are highly sensitive and some of them are medium sensitive. The sensitive data can regain only by the owner or someone the owner wishes to distribute the data. Public data can be accessed by everybody without any restriction. But in the matter of private message we include an extra component into the hybrid cloud named OTP generator for the verification function. The private messages are hidden inside a cover audio and generate a stego audio. The stego audio is accurately analogous to original audio. The trivial variation in the audio is barely discernible due to the masquerade upshot of Human Auditory System (HAS). This means that the feeble sounds are unnoticeable in the vicinity of large sounds. In cloud storage system as a replacement for of private data we store this stego audio. Except on behalf of public data we don't perform any amendment to store inside the cloud. Public data remains same in the cloud storage system. This can diminish the computational cost, storage and communication operating cost.

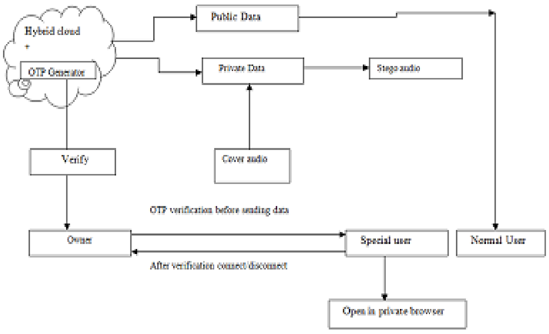

Fig: Proposed Approach

At some point in the time of decoding, the OTP generator sends a password to registered user for a substantiation purpose. When the owner act in response to that message he is redirected to a private browser. From here he be able to get the extracted message. So at this juncture the private message is only visible to the owner and the special user. This is a effortless and robust approach weigh against to other approaches.

Even though our approach is healthier we want to consider the deception of attacker. When he enters to our system he detects only the audio file. If he crashes the entire hybrid cloud we can secure our data by stopping the OTP generation service until the cloud recovered.

Basic Elements

The basic elements used by this system are:

DOI 10.17148/IJARCCE

- **Hybrid cloud:** Combination of public cloud provider by private cloud infrastructure. It can accumulate information with less cost contrast to private cloud and public cloud.
- **Owner:** Person has the consulate to upload and transform the content and upload the services.
- **User:** person who be capable of access the services and data uploaded by the owner.
- **Special user:** person who can retrieve the medium sensitive data contribute by the owner.
- **OTP generator:** One time password generator which is used for the authentication purpose.

Input Audio

Input audio is the cover audio which is used to put out of sight the data. This may be of several formats. While prefer the cover audio we want to think about the size of the audio file. For the reason that larger audio file consume extra bandwidth. At the same time as we use small audio file may leads to the loss of information for a massive size of data. So it is better to go for a medium size audio file.

Input Data

It is the text message which we would like to hide inside the audio. Here the original audio files are fragmented into frames. And then estimate the frame redundant bit. Subsequently select the content to embed and test out whether the frame can sustain the content. If yes then hide content into the frame to acquire the stego audio. This procedure continues until it reaches the end of file.

Algorithm for Encoding

- **Step1:** Original audio segment into frames
- **Step2:** Check whether the frame can bear the content want to embed.
- **Step3:** If yes embed some hidden content. Else select the next frame.
- **Step4:** If want to hide more content go to step 2.

Step5: If not create stego audio.

Algorithm for Decoding

- **Step1:** When request send OTP generator sends a password to the user.
- **Step2:** There establish a onetime connection, owner directed to a private browser.
- **Step3:** combine the frame segment and decode the original data.

CONCLUSION

In this paper I introduce a new approach to enhance the security of data in hybrid could. This can be obtained by hide the secret data inside a cover audio. This approach doesn't reveal the presence of the secret information. Steganography can be done on image, text, audio and video. Audio steganography is better than image steganography because it can hide more content than in image. Here the both public and stego data are stored in hybrid cloud. During the decoding OTP generator send a onetime password to owner for the verification purpose. Whether he is an authorized person he is directed to a private browser where he can get the original secret content. Comparing to other approaches this is more secure approach to store data inside a hybrid cloud. And also this is a simple approach to make secure the data. This system can be mainly used to hide the important formulas, or trade secrets in organizations. Even though it has much merit our system is vulnerable to ip spoofing. The advantage of this system depends on the efficiency of cover audio and the size of the text want to input.

ACKNOWLEDGMENT

I take this opportunity to express my gratitude to all who help me to complete my paper. I thank to god almighty for all his blessing during this endeavour. Then I thank to my guide, lectures, parents and my friends who help, guide, advice me during this period.

REFERENCES

[1] http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf. Hybrid cloud definition.

E. Zwicker and H. Fastl, Psychoacoustics, Springer Verlag, Berlin,

Fatiha Djebbar, Baghdad Ayady, Habib Hamamzand Karim Abed-Meraim*x* "A view on latest audio steganography techniques"2011 international conference on innovation on information technology.

Ronak Doshi, Pratik Jain, Lalit Gupta "Steganography and its application in security" International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638

[2] Jayaram P, Ranganatha H R, Anupama H S "Information Hiding Using Audio Steganography – A Survey" The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[3] Bo Liu, Erci Xu, Jin Wang, Ziling Wei, Liyang Xu, Baokang Zhao*, Jinshu Su "Thwarting Audio Steganography Attacks in Cloud Storage Systems" 2011 International Conference on Cloud and Service Computing.

Xueli Huang and Xiaojiang Du "Efficiently Secure Data Privacy on Hybrid Cloud" IEEE ICC 2013 - Communication and Information Systems Security Symposium.

[4] Aishwarya KauJ, Sheoli Tu1i, and Rachna Jain "Combining Encryption and Stego – Object Processing: A New Direction in Cloud Security".978-1-4799-3064-7/14/$31. 00©20 14 IEEE.

DOI 10.17148/IJARCCE