STEGANOGRAPHY IN CLOUD SECURITY: A REVIEW

Chandni[1] and Vikram Singh[2]

[1] M.Tech. CSE Scholar, Ch. Devi Lal University, Sirsa.

[1] Professor, Department of Computer Science, Ch. Devi Lal University, Sirsa.

Abstract: This article has reviewed the works wherein of steganography has been used in cloud computing. There are several communications reporting the use of steganography for securing data transmission over the cloud. The embedding of secret messages can be done efficiently and easily with the use of this technology. The encoding of the messages is done by computerized tools and these are hidden in another file. Several techniques used to secure the data transmission have been reviewed here.This communication has also discussed the limitations of steganography as used in the field of cloud security. The review work would be beneficial for those who need to understand the horizon of steganography based techniques as used to secure data transmission over the cloud.

Keywords Cloud computing, steganography, one-way hashing, information hiding.

1. INTRODUCTION

Cloud computing is a mechanism which provides many types of facilities that is more usable for us to transfer the data or any other information. It is the delivery of computing services. Various services are servers, storage, database, software, networking and analytics over the network. Many companies are offering these computing services. Such companies are called cloud service providers. They typically charge for cloud computing services based on usage. It is similar to how they billed for water or electricity at home. Working of Steganography is also discussed here, In the present time, it has been analyzed that the steganography performs along with an enhancement in secret bits in files. It is not easy to break it in order to make it extra attractive. It is effective technique to send the very important personal parallel to business data. Here the social channels have been used. (Singla, 2018).

1.1 Cloud computing

There are several advantages of cloud computing. Cloud computing provides several benefits. Operators on the Internet would be able to get remote applications as utilities. Cloud computing is offering online development tools. The operator can modify and configure application online at any time. Operators have been provided platform-independent availability of cloud resources which would be available over the Internet. Cloud computing is offering on-demand self-services& there is no necessity of interaction with the cloud-based service provider. Cloud computing usually works at high efficiency. It is not going to optimum utilization thus it is cost-effective highly. Cloud computing is more reliable due to the load balancing feature. Cloud computing has a feature of load balancing that indicates its reliability. The need for steganography is also presented here. It provides 24x7 support. Cloud computing required to pay as they use. It has a lower total cost of ownership. Cloud computing provides reliability, scalability, sustainability. It provides secure storage management expenditure. It is capable to free up internal resources. This type of systems has been considered highly automated. These systems have been dependent on utility. It offers quick and easy agile deployments. These types of systems are device and location independent (Bansal, 2016).

1.2 Steganography

The embedding of secret messages can be done efficiently and easily in the present computer age with the use of technology. The encoding of the messages is done by computerized tools and these are hidden in another file. Steganography is defined by Johnson as the method of hiding the occurrence of information in clearly harmless carriers. It also added that the encrypted message may raise suspicion whereas it is not arisen by a hidden message. Thus, it is concentrated that the fact should be concealed that there is the first place of the message. (Anderson and Petitcolas, 1998).

Working of Steganography is also discussed here, In the present time, it has been analyzed that the steganography performs along with an enhancement in secret bits in files. It is not easy to break it in order to make it extra attractive. It is effective technique to send the very important personal parallel to business data. Here the social channels have been used. (Wojciech, 2011).

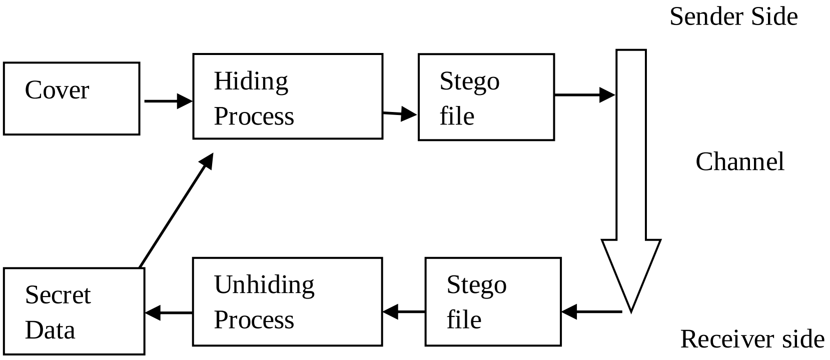

Figure1. Working of steganography

In the past time, it was used as a transformer of transmission. It has been assumed that the initial Greek used to cut the head hair of the message supplier. After that they locate the content of message on the head of messenger. After that, during the time taken by the messenger, his hair grew up. In this way the content situated on his hair becomes safe. After the progress of his hair, he passed the area of opponent without assuming. Not one can assume that precious data is located on the head of message. When the messenger reached near of data receiver, his head had been bald and got the message.

As different techniques have been developed and eliminate the process in whihch bald head has been used. Steganography's working process has been presented in this introduction part**.** In the present time, it has been analyzed that the steganography performs along with an enhancement in secret bits in files. It is not easy to break it in order to make it extra attractive. It is effective technique to send the very important personal parallel to business data. Here the social channels have been used.

One-Way Hashing

It is utilized for ensuring the third party has not messed about with the message which has been sent. Its accomplishment can be done by generating a hash of the message. It is done with the use of fixed character size for each item exist in the message. It has been indicated by sender and recipient that it has tampered.

Attaching Text to an Image

There is an attachment of explanatory notes with the image. There is the use of this technology in the medical profession. It has been used by one medical office transmits the graphic to separate medical office. If there is a requirement of explanatory notes by sending medical about the main focus of receiving a medical office, this work may be completed with Steganography.

Hiding Information

Steganography may also be utilized to guard the identities and valuable data by theft and viewing which is unauthorized. Another use is where there is potential sabotage by hiding the message by an unsuspicious image.

2. LITERATURE REVIEW

This section has summarised various researches related to the stenography in cloud data security. Liu (2011) has investigated the issue of thwarting audio steganography attacks in cloud storage systems. Their experimental results have shownthe scheme to be very efficient in thwarting the audio steganography attacks in cloud storage systems.

Wojciech(2011) has discussed cloud computing steganography proof. The paper focuses on the characterization of information hiding possibilities in cloud computing. The researcher has introduceda classification of steganographic communication scenarios in cloud computing which is based on the location of the stereograms receiver. These scenarios, as well as the threats that steganographic methods can cause, must be taken into account when designing secure cloud computing services.

Nimmy(2014) proposed the novel mutual authentication protocol. This protocol has been used in cloud computing. For this purpose, they used the secret sharing as well as the steganography. It has been analyzed that the proposed protocol offers the mutual authentication in users and cloud server. Also, the users are achieved the flexibility for changing the password. Therefore, the efficient security characteristics provide the protocol well suited.

Mandai (2015) proposed the research wrok on secret data sharing within cloud system appkying the mixup of steganography with encryption method. For this objective, steganography as well as the encryption with GA has been used. steganography with an innovative cryptograpy has been utilized. The steganographic method has embedded secret data with the use of Pixel Mapping Method. It has been determined that it has been done in a chaotic sequence. This sequence has been created by technique of chaotic map.

Prakash (2015) discussd the three-step data security model to perform in cloud computing with RSA and the data hiding technique steganography. The proposed model performs in cloud computing environment. The proposed model is dependent on RSA as well as on steganography. This research work has described a pattern to secure data and information in a cloud system. It is necessary to secure the data during data sharing and storing of data. For this in proposed work, they have used a pattern in which cryptography with steganography method has been involved.

Bansal (2016) analyzed the low error rate dependent protected sharing related to personal health record with in cloud environment applying DWT steganography. This considered sharing is of personal health record within cloud environment. For this, DWT steganography has been used. In the research work, the researcher has focused on enhancement of security related to the PHR. It has been by the implementation of DWT related to the Steganography. It has been analyzed that the Steganography can be defining as a process used to secure the information in the form of the graphical content. Steganography involves to the insert the huge size data in the graph form.

Maitri (2016) explained the protected file storage within cloud system. For this hybrid cryptography algorithm has been used. Cryptography and steganography has been known as well populated technique used to secure the data. The research has attempted to highlight the challenge faced during the formulation of a model to secure the data using image steganography. The proposed technique is an updated LSB image steganographic method. Here the password has been utilized to secure the data in an image.

Abduljabbar (2016) offered the research work on robust scheme to protect authentication code of message/image documents in cloud computing. A number of image/message document authentication and integrity schemes have been conducted to recognize any modification in the exchange of documents between two entities (sender and receiver) within a cloud environment.

Mittal (2016) explained the data security using RSA encryption combined with image steganography. They considered RSA algorithm for encryption and image steganography for data hiding using LSB technique. Ranjan (2016) wrote on advanced mechanisms to shared and protected cloud data with the use of multilayer steganography as well as the cryptography. The main focus of this system is to forestall information access from cloud data storage centers by unauthorized users.

Amalarethinam (2017) defined the provide the research work on data security increment in public cloud storage. For this, data obfuscation as well as the steganography has been used. Security of Data storage can be defined as issue faced during cloud storage. The results have proved that defined technique is more capacity with best quality of stego images.

El-latif (2018) discussed the necessesity of the security of quantum steganography protocol. In the research work, they presented an innovative framework to protect data within fog cloud IoT. The need for steganography is also presented here. It provides 24x7 support. Cloud computing required to pay as they use. It has a lower total cost of ownership. Cloud computing provides reliability, scalability, sustainability. It provides secure storage management expenditure. It is capable to free up internal resources. This type of systems has been considered highly automated. These systems have been dependent on utility.

Singla (2018) reviewed the cryptography and steganography algorithm for Cloud Computing. In this paper, firstly security attacks on cloud computing is discussed. To countermeasure these attacks, cryptography and steganography techniques are studied and critical analysis is done. The open research area defined on the basis of studies and critical analysis, which helps the other research to contribute their research in this field.

Ahmad (2018) provide the optimization of data hiding. This has ben done in complemented or may be non-complemented form within video steganography. The results of research work have shown that steganography used in proposed system is more effective than traditional state of the art methods. The updated algorithm had been setup. It is greatly effective in of video data within cloud environment.

AlKhamese (2019) proposed the data security in cloud computing using. Steganography and cryptography are some of the security techniques applied in the cloud to secure the user data transmitting. The objective of steganography is to hide the existence of communication from the unintended users; whereas cryptography encrypts the data to make it more secure.

3. STEGANOGRAPHY TECHNIQUES IN CLOUD SECURITY

On the base of several standards, Steganography technique has been categonized. The spatial domain indicates to the classification of graphics of spatial domain. There are different researches which considered the different technique of steganography. Techniques used in Traditional work has been discussed in the following paragraphs.

Nimmy (2014) has proposed a novel mutual authentication protocol has been discussed. In the proposed protocol, mutual authentication as well as establishment of session key between clients and server of cloud has been discussed. For this purpose, they used the secret sharing as well as the steganography. It has been analyzed that the proposed protocol offers the mutual authentication in users and cloud server. Also, the users are achieved the flexibility for changing the password. Therefore, the efficient security characteristics provide the protocol well suited. It has been used cloud system.

In (Mittal 2016) an RSA Encryption has been combined with image steganography. They considered RSA algorithm for encryption and image steganography for data hiding using LSB technique. Steganography and encryption combined enhance cloud security by providing dual layer protection to the data, as steganography aims at hiding the existence of the data itself and encryption prevents the correct interpretation of the data. They have taken into consideration RSA algorithm for encryption and image steganography for data hiding using LSB technique.

Ranjan (2016) has discussed a multilayer steganography and cryptography based system. The main focus of this system is to forestall information access from cloud data storage centers by unauthorized users. To make sure privacy of data in cloud computing, it planned an effective and a unique approach to make sure information security in cloud computing by means of encrypting and concealing the info with multimedia exploitation thought of multilayer steganography with advanced encryption standard (AES). The main focus of this system is to forestall information access from cloud data storage centers by unauthorized users. This theme perfectly stored information at cloud data storage centers and retrieves data from it once it's required. This gives the terribly high-level knowledge security for the online virtual system and saves the fraud users to use your knowledge (Ranjan 2016).

In (Maitri 2016), the researcher has used hybrid cryptography algorithm.Cryptography and steganography techniques are more popular now a day's for data security. The research has attempted to highlight the challenge faced during the formulation of a model to secure the data using image steganography. The proposed technique is an updated LSB image steganographic method. Here the password has been utilized to secure the data in an image. In this proposed model, different algorithms Advanced Encryption Standard, blowfish, RC6, as well as BRA algorithms has been applied. Such are used to offer the security block-wisely to the data. 128 bit is the key size of all algorithm. LSB steganography method has been discussed to provide the security of key information. Key data involves that part of the file is encrypted using by which algorithm and key. The file is split into eight parts. Each and every part of the file is encrypted using a different algorithm. All parts of the file are encrypted simultaneously with the help of multithreading technique. Data encryption keys are inserted into the cover image using the LSB technique. Stego image is sent to a valid receiver using email. For file decryption purpose reverse process of encryption is applied.

In (Bansal 2016), a low error rate based secure sharing of the personal health record in cloud computing has been considered. The researcher has used DWT steganography for this purpose. In this paper, the author has worked on enhancing the security of PHR by the implementation of DWT that is based over Steganography. Steganography is that process in which information can be hidden in a picture. Steganography has the ability to insert more information into one graphical content. The protocol has been formulated in a particular way.

In (Amalarethinam 2017), the researcher has used data obfuscation as well as the steganography also. Data storage security is very basic issue situated within cloud storage. For this, data obfuscation as well as the steganography has been used. Security of Data storage can be defined as issue faced during cloud storage. The results have proved that defined technique is more capacity with best quality of stego images.

In the research work, the researcher enhanced the steganography using K strange point clustering. In the research work the focus of researcher was to hide the data with in cloud environment. They considered the use of steganography by clustering. They provide the implementation using clustering algorithm named K strange point. The made the comparative analysis of K Means Clustering Algorithm with K strange Point. They also asserted that the used methodology is better than the K strange points clustering algorithm. I order to secure the data within covering medium theyhave usedthe LSB algorithm. They finally proposed an enhanced scheme for best hiding capacity (Pradesh 2017).

Ahmad (2018) has used the optimized data hiding in complemented or non- complemented form in video steganography. They have explained a steganography method able to get zero variability with low time for computational. It enable the user to be expressed proficiently to recipient. It has been done at the time of getting the secret data. The proposed algorithm performance had been assessed with the use of several parameters. Such parameters are PSNR, embedding capacity etc. The results of the research work has revealed that definedsteganography model is better than the existing state of the art techniques.

El-latif (2018) has stated the security of Quantum Steganography Protocol For Fog Cloud Internet Of Things. The research work has discussed an innovative environment to secure the data within fog cloud IoT. The intended receiver in another location accesses the data from the fog cloud and extracts the intended content via the proposed extraction approach. This paper also presents a novel quantum steganography protocol based on the hash function and quantum entangled states. To the best of their knowledge, there is no prior quantum steganography protocol that authenticates an embedded secret message. In the suggested protocol, the hash function is utilized to authenticate embedded secret messages. The presented protocol is secure against well-known attacks, such as message, man-in-the-middle, and no-message attacks (El-latif 2018).

4. CONCLUSION

The research work has proposed a review of steganography that is applicable to secure the data transmission over the cloud. There are several kinds of attack such as Timing attack, Brute force attack, a man in the middle attack, etc. Due to such attacks, data transmission over the cloud is not secure. In the past, there were several researchers that introduced a number of techniques to secure the data transmission over the cloud. Such techniques are as RSA, Encryption and decryption key as AES, DES, and 3DES. These techniques are efficient to secure the data transmission but in a limit. In the proposed model, the security of data a with security of network connection has been considered. Moreover, there is also focus on the performance of the system along with security. The research work would be applicable to provide the review of steganography along with other different techniques used to secure the data over the cloud.

REFERENCES

Liu,B., et al., "Thwarting Audio Steganography Attacks in Cloud Storage Systems," pp. 259–265, 2011.

Murakami K., Hanyu, R., Zhao, Q. and Kaneda, Y., "Improvement of Security in Cloud Systems dependent on Steganography," pp. 503–508, 2013.

Nimmy, K., "Novel Mutual Authentication Protocol for Cloud Computing applying Secret Sharing and Steganography," pp. 101–106, 2014.

Mandai, S., "Secret Data Sharing in Cloud Environment Applying Steganography and Encryption Using GA," pp. 1469–1474,2015.

Prakash, J. and Cse, M. T.,"Three Step Data Security Model for Cloud Computing dependent on RSA and Steganography Techniques," pp. 490–494,2015.

Bansal P., Sharma, B. and Saxena, M., "Low Error Rate Based Secure Sharing of Personal Health Record in Cloud Computing applying DWT Steganography," 2016.

Maitri, P. V.,"Secure File storage in Cloud Computing applying Hybrid Cryptography Algorithm," pp. 1635–1638, 2016.

Abduljabbar, Zaid Ameen,"Robust scheme to protect authentication code of message/image documents in cloud computing" 2016.

Mittal, S., Arora, S. and Jain, R., "PData Security using RSA Encryption Combined with Image Steganography," 2016.

Ranjan, A.,"Advanced techniques to shared & protect cloud data applying Multilayer Steganography and Cryptography," pp. 35–41, 2016.

Amalarethinam, D. I. G.,"Data Security Enhancement in Public Cloud Storage applying Data Obfuscation and Steganography," 2016.

Pradesh, U., Singh, R., Pradesh, U. and Pradesh, U., "Enhancement of Steganography Using K Strange Point Clustering" 2017.

El-latif, A. A. A., Abd-el-Atty, B., Hossain, M. S., Elmougy, S. andGhoniem, A., "Secure quantum steganography protocol for fog cloud Internet of Things," vol. 3536, no. c, pp. 1–8, 2018.

Singla, S. andBala, A., "A Review: Cryptography and Steganography Algorithm for Cloud Computing," 2018 Second Int. Conf. Inven. Commun. Comput. Technol., no. Icicct, pp. 953–957, 2018.

Ahmad, Z., "Optimized Data Hiding in Complemented or Non- Complemented Form in Video Steganography," 2018 Cyber Resil. Conf., pp. 1–4, 2018.

AlKhamese, A. Y. and Hanafy, I. M.,"Steganography: A Review," 2019 Int. Conf. Innov. Trends Comput. Eng., no. February, pp. 549–558, 2019.