**PROJECT TOPIC**

**Data security on the cloud: Steganography**

***Authors:*** *Scott Anderwald, Olufemi Adesanya and Marvin Scott*

Data security on the cloud: Which encryption method is the best.

**Abstract**:

Data security as we have seen is a never-ending issue with businesses and individuals. As the amount of data increases on the cloud data security will be a constant issue. Steganography is one method of data security. This method allows data to be hidden in files or image. The method of hiding data within files should allow for a more secure way to store data. This paper will explore the possibilities of steganography for the use in data security in the cloud.

1. **Introduction**:

As the amount of information increase on a daily basis, storage has become a major problem with many businesses and individuals. Onsite databases storage system, while they still have pivotal role in any organization data system flow has started to overwhelm their capabilities. To aid in the issue of storage a system of “cloud storage” has been developed. Like many data storage systems, the issue of data security needs to be addressed.

Businesses and individuals need to have the confidence that what data is being stored for them is secure. A system of security where data is hidden to conceal its information has been purposed. Steganography is the process of hiding data within another file or image. The method needs to be further studied to determine if it would be viable method for data security on the cloud.

Data security in the cloud computing is more perplexed than data security in the traditional information systems.

To make the cloud computing be adopted by users and enterprise, the security concerns of users should be rectified first to make cloud environment trustworthy. The trustworthy environment is the fundamental prerequisite to win confidence of users to adopt such a technology. Latif et al. discussed the assessment of cloud computing risks.

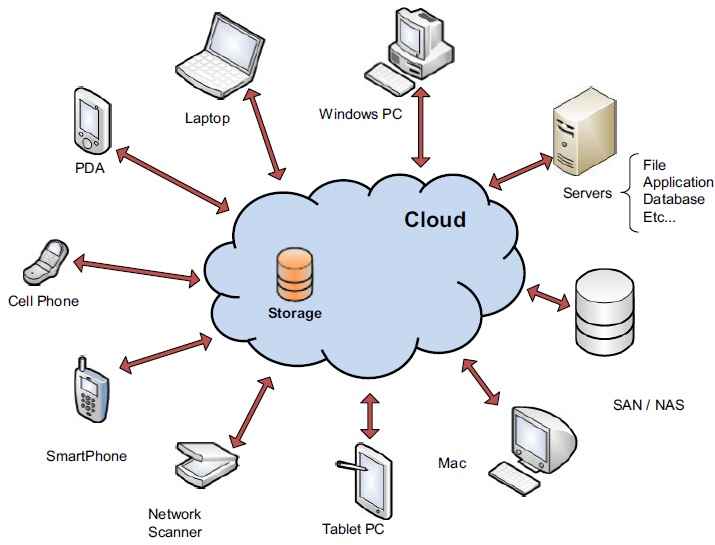
Afore the data security issues are discussed, the functions of cloud computing are analyzed first. Cloud computing is additionally kenned as on-demand accommodation. In the cloud computing environment, there is a cloud accommodation provider that facilitates accommodations and manages the accommodations. The cloud provider facilitates all the accommodations over the Internet, while end users use accommodations for slaking their business needs and then pay the accommodation provider accordingly.

1. **Cloud** **storage**

With the increasing amount of mobility in the world people are looking for the cloud to be able to share files. Per the Techradar website best provides for 2017 include: Drobox, Google Drive, Mega, OneDrive, ICloud, Box, NextCloud, SpiderOak, IDrive, pCloud. While there are many advantages to using the cloud, storage including Usability, Bandwidth, Accessibility, Disaster Recovery, and Cost savings (Baylor University Document) security is one of many disadvantages.

Cloud storage is a system where data is stored remotely by a service provider that maintains access to all user who have access to the data. This system not only stores the data but provides management and backup of all files.

Fig 1. Diagram of How Cloud Storage Works.

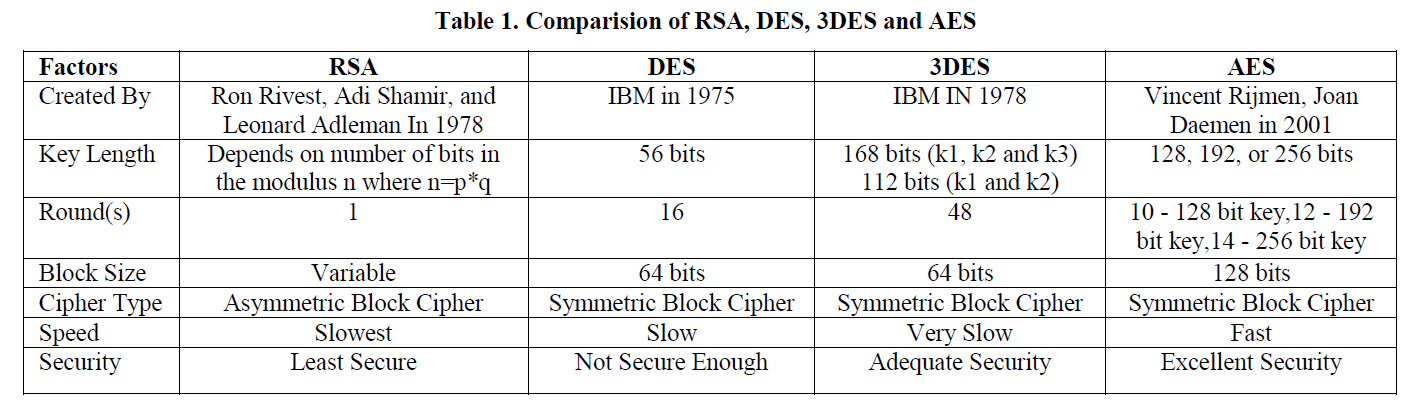


With this convenience come the possibility of actors by intentionally or not hacking into the system. This leave the questions which encryption method would work on the cloud.

For the cloud, there is three types of systems we can utilize. The first being which the public cloud. Public cloud is accessed “via interfaces using mainstream web browsers” ref 6 Of the three the “Public clouds are less secure than the other cloud models because it places an additional burden ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.” Ref 6. This should concern many who place documents and pictures both of which can be private in nature on systems like IClouds and other various public systems. The next system would be the private systems and can be “set up within an organization’s internal enterprise datacenter. The private cloud system is different since the “Cloud resources and applications are managed by the organizations itself, like Intranet functionality” ref 6. The last is the Hybrid system which is “is a private cloud linked to one or more external cloud services, centrally managed provisioned as a single unit, and circumscribed by a secure network. Many types of encryption to assure data security on the cloud has been explored one such being explored is Steganography.

1. **Encryption Methods.**

Several methods for encryption exist for the security of data on the network. There are two main types of encryption symmetric and asymmetric key. Symmetric involves the use of a shared key system where both parties have the same key. Asymmetric which is also referred to as public key contains different key one for encryption and another for decryption. Per a study by Singh, Supriya they stated that “Asymmetric encryption techniques are about 1000 time slower than symmetric encryption which makes it impractical when trying to encrypt large amounts of data”. Please see table one from the study



From the paper by Khalid Alshafee titled “Encryption Techniques in the cloud” where he explored many other types of encryption methods including Identity-Based Encryption, Attribute-Based Encryption, and Fully Homomorphic Encryption stated that “Asymmetric and symmetric encryption alone is not enough to fulfill the security needs over the cloud atmosphere. There should be a combination of more than one cryptographic techniques to provide tight security of data over cloud. The very common and generic encryption”. With this more than one method should be utilized with data being stored on cloud servers. One such method being considered is steganography.

There is some hesitation about the use of steganography is the cloud environment. This hesitation is due to actors conducting nefarious deeds not in the interest of the public. In paper by Mazurzk, Szczypiorski titled “Is Cloud Computing Steganography-Proof” they stated “Stenographic techniques can be sued to provide a perfect tool for data exfiltration, to enable network attacks or hidden communication among secret parties”. While they might valid point in regards to various criminal activities including communications among varies terrorist cells. There could be cases of this occurring but could the actors find other means to pass along information by other means of encryption? Yes they could. Later stated in the paper by Mazurzk and Szczypiorski “ To conclude, cloud computing as a carrier for secret communication is not very different from any other popular steganographic carriers e.g. Like IP Telephony”.

1. **Steganography**

Steganography is an art of obnubilating data in a covered media (image, audio, video, text). In Steganography, we obnubilate the mere presence of that it will be undetectable. The covered media is culled in such a manner that it has capacity to obnubilate the data and robustness that provides quality to the stego image. As in the upcoming years the desideratum of data obnubilating, copyright bulwark, and confidentiality increases, steganography plays a consequential role in this field because of its some unique features. In this paper, we fixate on the different steganography methods. This review paper provides some consequential information about steganography methods that will avail in future researches in steganography and data obnubilating field. This paper is divided into different sections in which we explicate steganography system, cognate work, different steganography methods and conclusion.

The art of concealment can be used for many different things. For example, camouflage, has been used for years as a mean of for which people and or equipment can be hidden from their adversaries. Likewise, information can be hidden within for an example a picture. Chuck Easttom the author of Modern Cryptography stated that “Steganography is the art and science of writing a hidden message in such a way that no one, apart from the sender and intended recipient, suspects the message exists; it’s a form of security through obscurity”

1. **Steganography Methods**

Steganography is differentiated on the substructure of the media in which we obnubilate the data. These are: text, image, audio and video.

A. Text Steganography

The Steganography method utilizes the text media to obnubilate the data kenned as text Steganography. There are different techniques to embed the secret data in text files.

• Format Predicated Method

• Desultory and Statistical Method

• Linguistics Method

Format Predicated Method: This method modifies the subsisting text to obnubilate the data in such a manner that it involves the insertion of spaces, resizing the text, transmute the style of text.

Arbitrary and Statistical Method: In this method characters are obnubilated that appeared in desultory sequence. Statistical method determines the statistics such as mean, variance and chi square text which quantification the amount of redundant information to be obnubilated within the text.

Linguistics Method: It is the amalgamation of syntax and semantics. Syntactic steganalysis ascertain the correct structure as the text is engendered from grammar. In semantic method value is assigned to synonyms and data can be encoded to the authentic word of text.

B. Audio Steganography

When secret data is embedded into digital sound, the technique is kenned as audio steganography. This method embeds the secret message in WAV, AU and MP3 sound files. There are different methods through which audio steganography explored:

• Low Bit Encoding

• Phase Coding

• Spread Spectrum

Low Bit Encoding: This method is utilized by pitch period presage is conducted during low bit verbalization encoding. Thus, maintaining synchronization between information obnubilating and verbalization encoding.

Phase Encoding: In this method, stream file splits audio into blocks and embed whole secret sequence into phase spectrum of the first block.

Spread Spectrum Encoding: One particular method of spread spectrum encoding is DSSS (Direct Sequence Spread Spectrum) which spread steganography by multiplying it by certain pseudorandom sequence.

C. Image Steganography

In this method, images are utilized as cover object. The image Steganography, data obnubilating method can be relegated into different categories. These are spatial domain, frequency domain, and adaptive domain.

Spatial Domain Steganography: In spatial domain, cover image and secret data modified by utilizing LSB and level encoding. First, the cover image is decomposed into bit planes and then LSB is of bit planes superseded with secret data fit. LSB supersession is the mostly used steganographic technique. This supersession concept includes embedding at the minimum weighting bit as it will not affect the value of pristine pixel. Luon Ching Lin [5] proposed a scheme of data obnubilating in spatial domain with tolerance of distortion. This method provides better image quality. The only drawback of the LSB insertion is the simplicity of extraction process. Thus, a secret listener can facilely extract the data that we are sending.

Frequency Domain Steganography: In frequency domain, secret data is obnubilated in consequential areas of covered image, which makes data invigorate to attacks such as compression, cropping or image processing methods than LSB approach. This provides an enhanced security level to steganography method and lead to the development of algorithms. This method transforms include DCT, DWT and DFT. A lossless and reversible scheme have been introduced that use each block of quantized DCT coefficient in JPEG image for secret data [6]. The method results in high stego image quality and achieves reversibility. DCT coefficients of an image utilized for embedding data bits. F5 embeds data in DCT coefficient by rounding the quantized coefficients to the most proximate data bit.

It additionally uses matrix encoding for reducing the embedded noise in the signal. F5 is one of the most popular embedding schemes in DCT domain. Wavelet Transform (WT) converts spatial domain information to the frequency domain information. Wavelets are utilized in image because wavelet discretely partitions the high frequency and low frequency information pixel by pixel. This scheme mainly addresses the capacity and robustness of the data obnubilating system.

In recent year, DWT predicated algorithm for image has been proposed. These algorithms use CH band of cover image for obnubilating secret data.

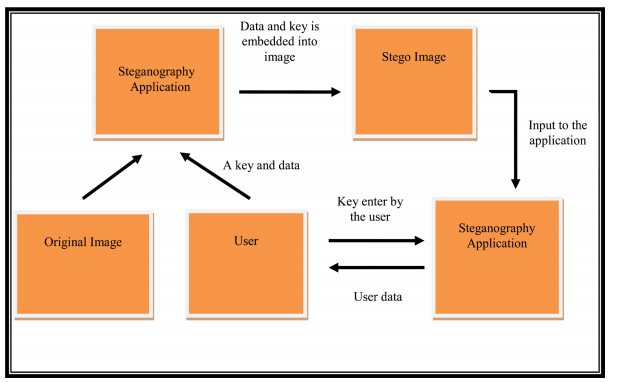
Adaptive Steganography: This steganography method is a special case of two methods: spatial domain and transform domain. It is additionally kenned as “Statistics Vigilant Embedding” and “Masking”. Ecumenical features of images are utilized afore embedding secret data in coefficients of DCT or DWT. This statistics will decide where changes can be made.

1. **Step involved for Steganography.**

Steganography can be applied in various way. By hiding data in plain sight this method could include according to Reza, and Sonawane where the data is

1. Encrypted which is optional
2. Data chunking
3. Application of steganography
4. Combination of Files
5. Decryption which is also optional.

From there paper the following workflow for the encryption.



1. How would it work and the advantages?

“It works by replacing bits of useless or unused data in regular computers files(such as graphics, sounds, text, etc.) with bits of different visible information” Ahamad and Aljumuh. Mention before it’s basically camouflage for data. Steganography is not really encryption the data is hidden in plain sight. So, potentially it would usefully as Ahamad and Aljumuh stated where encryption could not be used.

1. **Conclusion**

By placing data within an image coupled with an encryption method this would allow for data storage within the cloud to be safer for all parties. The client (user) could hopefully be somewhat satisfied about the security of the data while the owners of the cloud could be less concerned about the possibility of legal issues with data security.

References

1 <http://www.techradar.com/news/top-10-best-cloud-storage-services-of-2017>

2 <http://www.baylor.edu/business/mis/nonprofits/doc.php/197132.pdf>

1. <https://www.cloudwards.net/cloud-storage-good-idea/>

4.<http://brisjast.com/wp-content/uploads/2015/11/MRR-July.-12-2014.pdf>

5. “The Managent of Security in Cloud Computing, Ramgovind S, Eloff MM, Smith, 2010

6. “Encryption Techniques in the Cloud” Alshafee Khalid 2016

7. N. F. Johnson, S. Jajodia, “Exploring Steganography: Seeing the Unseen”, IEEE Computer vol. 31, issue 2, pp. 26-34, 1998.

8 Artz D., “Digital Steganography: Hiding Data within Data”, Internet Computing IEEE, vol. 5, issue 3, pp. 75-80, 2001.

9. L-C. Lin, “Hiding Data in Spatial Domain with Distortion Tolerance”, Computer Standard & Interfaces 31, pp. 458-464, (2009).

10. Provos N. and HoneymanP, “Hide and Seek: An Introduction to Steganography”, IEEE Security and Privacy, vol. 01, issue 3, pp. 32-44, May-June 2003.

11. ShavetaMahajan, Arpinder Singh, “A Review of Methods and Approach for Secure Steganography”, International Journal of Advanced ResearchComputer Science and Software Engineering, vol 2, issue 10, pp. 67-70, October 2012.

12. C-C. Chang, “Reversible Hiding in DCT based Compressed Images”, Information Sciences 177, pp. 2768-2786, (2007).

13. Easttom, Chuck. (2016) Modern Crytography. New York, etc. McGraw Hill