# A Review of Privacy Protection of Cloud Storage and Steganography Techniques

**Alok Ranjan**[1], **Mansi Bhonsle**[2]

[1]PG Scholar, Department of Computer Engineering, G. H. Raisoni College of Engg. and Mgmt., Pune, India-412 207

[2]Assistant Professor, Department of Computer Engineering, G. H. Raisoni College of Engg. and Mgmt., Pune, India-412 207

**Abstract:** ***Cloud computing is one among the most recent growing area in the field of IT industry also called on-demand computing. The growth in field of cloud computing can increase threat security aspects. So security has remained a relentless concern for day today usage of internet, networking and cloud computing is affected. However the general public communication channels are liable to security attacks that may cause unauthorized access to some info. Encryption has been accustomed persist and forestall these attacks. However once the data is decrypted it'll be exposed to the attackers once more and it'll not have any security protection. Steganography is that the science of embedding the secret information among different medium files (text, audio, image, and video) during a method that hides the existence of the secret message at all. This paper provides the details of Cloud computing and steganography presents with a quick review of cloud services, trust, privacy, security and also projected numerous steganography techniques recently introduced by various researchers around the globe. The main motive of concerning this paper is to make more secured your cloud data and also introduce the technique to make it better approach. So that user has full trust on cloud data. Hence, it provides responsibleness, measurability, high performance and relatively low value feasible solution as compared to devoted infrastructures.***

**Keywords:** Cloud Computing, Cloud Services, Data-centers, Encryption, Hybrid Cloud, Steganography, Third Party Auditor (TPA).

## 1. Introduction

The paper will mainly focus on Cloud security with your confidential data. For dealing this term, we've discussed various terminologies but mainly focus on two terms such as "Cloud Computing" and "Steganography". Also, we've explained about the how security can be enhanced the cloud security data using steganography. We've also walk through about different kind of cloud services and current issue, challenges and Methods.

### 1.1. Cloud Computing

Cloud computing one of the fast growing field in IT industry because of various functionality which makes very easy life in terms of work. Before going into deep into cloud, then first let me introduce the exactly what is cloud? For answering this question, very simple manner. "Instead of saving everything in your local machine, save somewhere itself and access your information the same manner via internet." Cloud is not limit with your personal PC but we can access this service with any device where you can access internet as shown in fig.1.

The fundamental idea of cloud computing originated within the 1950s, once companies and learning institutes prioritized the potency of their large-scale mainframe computers, permitting multiple users each physical access to the pc from multiple terminals also as shared central process unit time. However it extremely wasn't till the past decade roughly that cloud computing extremely began to change into the behemoth. We all know these days, after the long dot-com, finally the development of cloud computing has e-trail with in 2000s by big company like Amazon and really they played a vital role for enhancing the functionality.

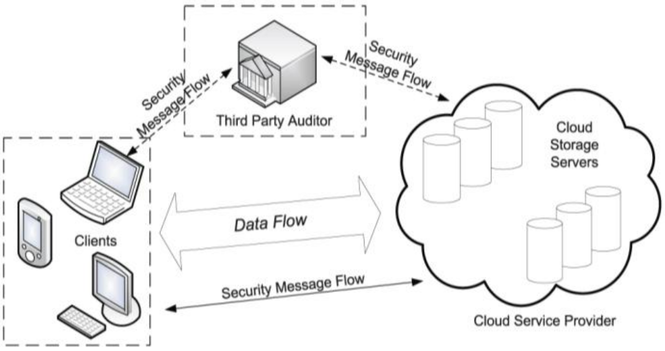

**Figure 1:** The Architecture of Cloud Data Storage Service

This accessibility of high-capacity networks and affordable computers, along with the widespread adoption of virtualization and service-oriented design. In this paper the focus on cloud computing overview to enhanced the cloud data security and why it become more popular in now-a-days. How cloud computig providing data privacy, Trust and security for cloud users. It will also give you better understanding about the confidentials information hinding technique using steganography.

### 1.1.1 Cloud Deployment Models

**Table1:** Types of Cloud and Related Associations

| *Deployment model* | *User* | *Accomplished By* |
|---|---|---|
| Private cloud | Private association | An organizations or a third party. |
| Public Cloud | General public or a large industry group. | An organization or selling cloud services. |
| Hybrid Cloud | Combination of multiple clouds (private, community, or public ) | An specifics organization or a third party vendor |
| Community Cloud | Shared by several groups and supports a specific community. | An organization or selling cloud services. |

### 1.1.2. Cloud Services

### A. Types of Cloud Computing

Cloud computing infrastructure providers provide leverage cloud computing for access to software [5], development platforms and physical hardware as shown in fig.2. These assets become virtualized and available as a service from the host these services can be classified in three categories [4].

a) **Saas:** Software-as-a-Service provides an application and Information service on cloud, this type of cloud is referring to a business-level service. Typically available over the public Internet (Google App Engine).

b) **PaaS:** Platform-as-a-Service provides development service on cloud; cloud development platforms enable application authoring and provide runtime environments without hardware investment (Windows Azure).

c) **IaaS:** Infrastructure-as-a-Service provides Infrastructure services on cloud, this type of cloud enables IT infrastructure to be deployed and used via remote access and made available on an elastic basis (Amazon Web services).

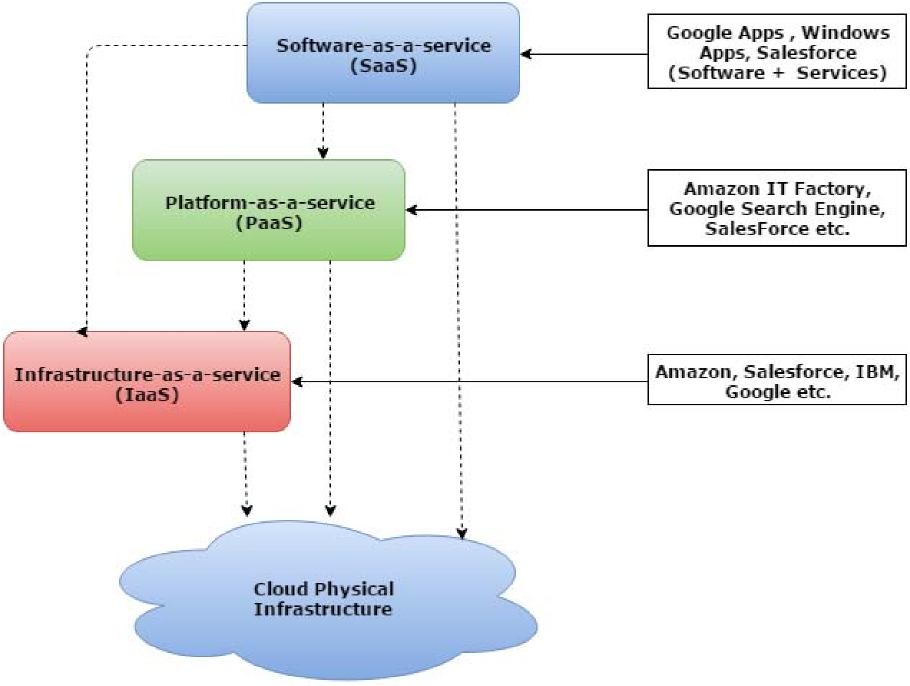
Software-as-a-service (SaaS)
Google Apps , Windows Apps, Salesforce (Software + Services)
Platform-as-a-service (PaaS)
Amazon IT Factory, Google Search Engine, SalesForce etc.
Infrastructure-as-a-service (IaaS)
Amazon, Salesforce, IBM, Google etc.
Cloud Physical Infrastructure

**Figure 2:** Different kind of Cloud Service Model

The above characterization is very much acknowledged in the business. David Linthicum depicts a more granular grouping on the premise of administration gave. These are:

i) Backups-data-as-a-service
ii) DB-as-a-service
iii) Information-as-a-service
iv) Process-as-a-service
v) Application-as-a-service
vi) Remote-Platform-as-a-service
vii) Integration-Service-as-a-service
viii) Security/Privacy-as-a-service
ix) Administration/Governance-as-a-service
x) Testing-as-a-service

### 1.2 Steganography

Steganography is be a Greek work which implies the covered writing. Steganography is associate art of hiding data in an exceedingly covered media (image, audio, video, text). In Steganography, we have a tendency to hide the mere presence of that it'll be undetectable and basic process as shown in fig.3. The lined media is chosen in such a fashion that it's capability to cover the information and hardiness that has quality to the stego image. As within the future years the requirement of knowledge activity, copyright protection, and confidentiality will increase, steganography plays a crucial role in this field as a result of its some distinctive options. In this paper, we have a tendency to specialize in the various steganography strategies.

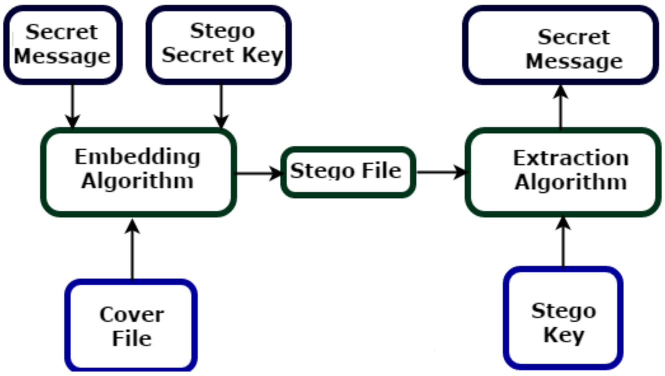

**Figure 3:** Architecture for Steganographic model

Steganography thus not only emphasize on the art of hiding information but also the art and science of hiding the communication that take place [14]. First applications of Steganography were documented by Herodotus, a Greek historian. During the century, the methods of using invisible inks were extremely popular [16]. During the World War II where people used ink for writing hidden messages, this was true [15]. The mixture will turn darker and the written message becomes visible upon heating. After some time, the Germans introduced the microdot technique where microdots are considered as photographs as small as a printed period, but with a clear format of a typewritten page [13, 20]. They were included in a letter or an envelope, and because of their tiny sizes, they could be indiscernible. Microdots were also hidden in body parts including nostrils, ears, or under fingernails [14].The military and several governmental agencies are looking into steganography for their own secret transmissions of information.

### 1.2.1. Types of Steganography

1) **Text Steganography:** It consists of concealing data within the text files. In this methodology, the key data is hidden behind each ordinal letter of each words of text message. Numbers of ways are accessible for concealing knowledge in document. These ways are i) Format based mostly methodology; ii) Random and statistical Method; iii) Linguistics Method.
2) **Image Steganography:** It concealing the info by taking the duvet object as image is referred as image steganography. In image steganography element intensities are accustomed hide the info. In digital steganography, pictures are widely used cover source as a result of there is range of bits presents in digital illustration of a picture.
3) **Audio Steganography:** It involves concealing data in audio files. This methodology hides the info in WAV, AU and MP3 sound files. There are completely different ways of audio steganography. These ways are i) Low Bit encryption ii) phase coding iii) spread Spectrum.
4) **Video Steganography:** it's a method of concealing any kind of files or data into digital video format. In this case video (combination of pictures) is employed as carrier for concealing the info. Typically separate trigonometric function transform (DCT) alter the values (e.g., 8.667 to 9) that is employed to cover the info in every of the images within the video, that is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

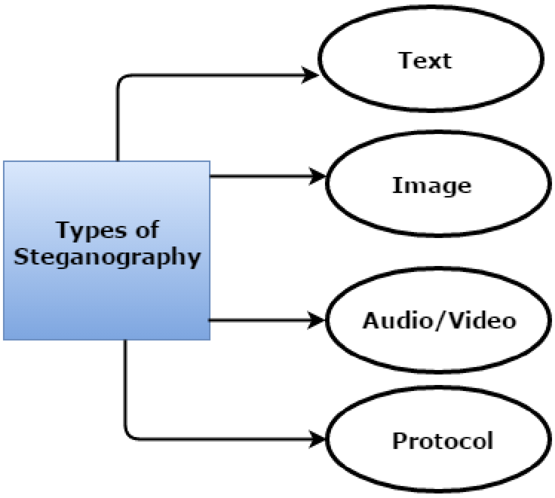

**Figure 4:** Classification of various types of steganography

**Network or Protocol Steganography:**
It involves concealing the knowledge by taking the network protocol like TCP, UDP, ICMP, IP etc., as cover object. In the OSI layer network model there exist covert channels wherever steganography are often used.

### 1.2.2. Steganography Techniques

**A. Spatial Domain Methods:** In this technique the secret information is embedded directly in the intensity of pixels. It means that some pixel values of the image are modified directly throughout hiding information. spatial domain techniques are classified into following categories: i)Least significant bit (LSB) ii) pixel value differencing (PVD) iii) Edges based} information embedding technique (EBE) iv) Random pixel embedding technique (RPE) v)Mapping pixel to hidden data technique vi) Labelling or connectivity method and vii) pixel intensity based.

**i. LSB:** In this technique the embedding is finished by commutation the least significant bits of image pixels with the bits of secret information. The image obtained after embedding is nearly the same as original image as a result of the modification in the LSB of image pixel doesn't bring too much variations in the image.

**ii. PVD:** In this technique, 2 consecutive pixels are designated for embedding the information. Payload is set by checking the distinction between 2 consecutive pixels and it serves as basis for distinctive whether or not the 2 pixels belong to a grip space or smooth area.

**B. Spread Spectrum Technique:** In this methodology the secret data is spread over a good frequency bandwidth. The quantitative relation of signal to noise in each frequency band should be therefore tiny that it become tough to discover the presence of information. Even if parts of information are off from many bands, there would be still enough data is present in different bands to recover the data.

**C. Statistical Technique:** In the technique message is embedded by changing many properties of the cover. It involves the ripping of cover into blocks and then embedding one message bit in every block. The cover block is changed only if the scale of message bit is one otherwise no modification is needed.

**D. Transform Domain Technique:** In this technique; the secret message is embedded within the transform or frequency domain of the cover. This can be an additional advanced approach of hiding message in a picture. There is a different algorithms and transformations are used on the image to hide message in it. The transform domain techniques are loosely classified like i) discrete Fourier transformation technique (DFT) ii) discrete cosine transformation technique (DCT) iii) discrete wavelet transformation technique (DWT) iv) lossless or reversible technique (DCT) and v) Embedding in coefficient bits.

**E. Distortion Techniques:** In this technique the key message is hold on by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the variations between the initial cover and the distorted cover to discover the sequence of modifications and consequently recover the key message.

**F. Masking and Filtering:** These techniques hide data by marking a picture. Steganography only hides the data wherever as watermarks becomes a beverage of the image.

These techniques inserted the data in the more significant areas instead of hiding it into the amplitude level. The watermarking techniques can be applied without the concern of image destruction due to lossy compression as they're additional integrated into the image. This methodology is basically used for 24-bit and grey scale pictures.

## 2. Related Work

***An Efficient Certificate less Encryption for Secure Data Sharing in Public Clouds [1]***

Here the authors give a really solid technique of maintaining the integrity of information. In this paper, first data is getting encrypted with Mediated certificateless public key encryption (mCL-PKE) scheme without using pairing operations which help to secure the data on public cloud. For getting back, based upon successful authorization, the cloud partially decrypts the encrypted data for the users and vice-versa.

***Cloud Information Security Using Third Party Auditor and Cryptographic Concepts [2]***

In this paper the authors has mainly focus an abstract view of different schemes proposed in recent past for cloud data security using Third party Auditor (TPA). The proposed model of the scheme in which the (TPA) will not have any kind of data stored in it. It will just maintain the log of each incoming request and outgoing response through Message Digests i.e. as its name suggests it will just audit all the transactions happening, and as the data encryption/decryption is done at client side only this scheme also solves the problem of integrity.

***Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding [3]***

In this paper, the authors have deal about the storage system with new technique. The proposed system considering a cloud storage system that consists of storage servers and key servers. We need to integrate a newly the proposed threshold proxy re-encryption scheme and erasure codes over exponents. The threshold proxy re-encryption theme supports secret writing, forwarding, and partial decipherment operations in an exceedingly distributed method. By using the threshold proxy re- encoding scheme, we have a tendency to present a secure cloud storage system that gives secure information storage and secure data forwarding practicality in a redistributed structure.

***Robust Data Security for Cloud while using Third Party Auditor [4]***

This paper discussed about the cloud computing security specially when data is in the plain format and also points that, how we can make data much more secured. Here, it present some way to implement Third Party Auditing (TPA) who not only check the re-liableness of Cloud Service provider (CSP) however additionally check the consistency and accountability of information. It also addresses this challenging open issue of integrity and data dynamics.

***Spatial Domain Image Steganography based on Security and Randomization [5]***

The objective of the paper is to increase the capacity of hidden data in a way that security could be maintained. Here they have introduced the technique called steganography. The Proposed method is achieving highest capacity among all existing methods without any distortion in image. When proposed method has been performed on different images, it has given constant result but other existing methods gave different results on different images.

***A Review on Steganography Methods [6]***

The authors of this paper have review about all steganography methods and how it's much more secured while traveling your data into network. This paper provides an overview of different steganography methods that satisfy the most important factors of steganography design. Moreover, this also explores the different method of data hiding: image steganography, audio steganography, video steganography, text steganography, steganography in spatial domain, transform domain and adaptive steganography.

***Capacity of Steganographic Channels [7]***

In this paper, it deals regarding the "how much information will safely be hidden without being detected?" For respondent this question, the planned technique uses an information-spectrum approach that permits for the analysis of absolute detection functions and channels. This provides machinery necessary to investigate a really broad vary of Steganographic channels. This approach permits for the analysis of absolute steganalyzers further as nonstationary, non-ergodic encoder and attack channels.

## 3. Security Issues, Challenges and Methodology

### 3.1 Factor affecting for cloud Users

Normally the cloud users can have differing types of logins, however it'll direct to the authentication problem. The only sign up provides the user level authentication. To extend the info handiness by using dynamic cloud storage servers among the cloud infrastructure proper intrusion prevention and detection elements are enforced with virtual firewall and IPS should be put in to protect the cloud network. In addition, the single management console is used for safeguarding the cloud network. The virtual management clients are Virtual Network Computing (VNC), Secure Shell (SSH) protocol, Secure Sockets Layer (SSL) protocol.

### 3.2 Challenges of Existing Cloud Computing Solutions

Like any new mechanism of technology, we tend to must address some challenges that cloud computing poses before we are able to acknowledge its full value, these includes lack of interoperability. The word interoperability is combination of 2 terms internal and portability, which means of the term movability, is ability to move a system one platform to another thus it provides the feature of internal movability capability to the cloud infrastructure; the cloud ability has the nice attention in literature.

The absence of standardization across cloud computing platforms creates unneeded complexness and leads to high shift costs. Every compute cloud vendor incorporates a completely different application model, several of that are proprietary, vertically integrated stacks that limit platform selection. Customers don't wish to be locked into one supplier and are usually reluctant to relinquish management of their mission-critical applications to hosting service providers.

### 3.3. Factors Affecting a Steganographic Methodology

The effectiveness of any Steganographic methodology may be determined by comparing stego-image with the cover Image. There are some factors that determine the potency of a method. These factors are:

1) **Robustness:** Robustness refers to the power of embedded data to stay intact if the stego- image undergoes transformations, like linear and non-linear filtering, sharpening or blurring. In addition of random noise, rotations and scaling, cropping or devastation, lossy compression.
2) **Imperceptibility:** The physical property means that invisibleness of a Steganographic algorithmic rule. It's the primary and foremost demand, since the strength of steganography lies in its ability to be ignored by the human eye.
3) **Payload Capacity:** It refers to the number of secret info which will be hidden in the cover source. Watermarking sometimes embed only a little quantity of copyright info, whereas, steganography focus at hidden communication and thus have comfortable embedding capability.
4) **PSNR (Peak Signal to Noise Ratio):** it's outlined as the ratio between the utmost possible power of a symptom and also the power of corrupting noise that affects the fidelity of its illustration. This ratio measures the standard between the original and a compressed image. The upper value of PSNR represents the higher quality of the compressed image.
5) **MSE (Mean sq. Error):** it's outlined as the average squared difference between a reference image and a distorted image. The smaller the MSE, the additional efficient the image steganography technique. MSE is computed constituent-by-pixel by adding up the squared variations of all the pixels and dividing by the entire pixel count.
6) **SNR (Signal to Noise Ratio):** it's the ratio between the signal power and also the noise power. It compares the amount of a desired signal to the level of background noise.

### 3.4. Solution for Steganographic Methodology with cloud:

If users try to saved, stored and share cloud data with stego-technique then the information will become highly confidential. There will be no chance for loss information for any point of view until the sender and receiver has licked the information. Using this technique, each user can access the information across the globe without any data loss.

## 4. Benefits and Applications

- The main benefits of cloud computing using across various platform in terms of i) Scalability, ii) Improved reliability, iii) Less infrastructure costs, iv) Enhance utilization, v) Improve end-user productivity, vi) Highly secure and vii) ) Energy efficient.
- The main benefits of the steganography is used to hiding the secret information with any kind of multimedia items and share, save and store your confidential data across the globe. The most benefits is using this technique, only sender and receiver are able to get the actual information.
- It is used mainly in almost all IT company such as Amazon, Google, Microsoft, Salesforce and so on for providing and getting service from provider to enhance the data portability, Remote IT infrastructure and backups for future purpose.
- It is used mainly in i) Copyright Protection, ii) Feature Tagging such as Captions, annotations, time stamps, iii) Secret Communications iv) Digital Watermark and also v) Uses by terrorists.

## 5. Conclusion

In this paper we have a tendency to present brief review of cloud computing that scope is huge in space of knowledge technology accessible by everybody. Here we tend to describe cloud threats, benefits, challenges, provides reliability, scalability, high performance and relatively low value feasible resolution as compared to devoted infrastructures. Here we main focus on security privacy and trust and publically cloud infrastructure. In the past few years, Steganography has become an interested field of information hiding techniques. This paper provides an outline of various steganography strategies that satisfy the foremost important factors of steganography design. These are un-detectability, capability and robustness.

## References

[1] Seung-Hyun S. and Xiaoyu D., "An Efficient Certificate less Encryption for Secure Data Sharing in Public Clouds", *IEEE Trans. on Knowledge And Data Engineering, Vol. 26, No. 9, Sept 2014.*

[2] Imran H. S., Bhagyashree B. R., "Cloud Information Security Using Third Party Auditor and Cryptographic Concepts", *International Journal of Application, Vol. 3, Issue 11, Nov 2014.*

[3] Hsiao-Ying L., Wen-Guey T., "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", *IEEE Trans. on Parallel and Distributed Systems, Vol. 23, No. 6, June 2012.*

[4] Abhishek Mohta, Ravi Kant Sahu and LK Awasthi, "Robust Data Security for Cloud while using Third Party Auditor", *IJARCSSE, Vol No. 2, Issue 2, Feb 2012.*

[5] Namita T., Dr. Madhu Sandilya and Dr. Meenu Chawla, "Spatial Domain Image Steganography based on Security and Randomization*", IJACSA, Vol. 5, No. 1, 2014.*

[6] Rakhi and Suresh G., "A Review On Steganography Methods*",IJAREEIE, Vol. 2, Issue 10,* October 2013

[7] Jeremiah J. H. and William A. P., "Capacity of Steganographic Channels", In proceeding with IEEE Transactions on Information Theory, Dec. 2012.

[8] X. Zhifeng and X. Yang, "Security and privacy in cloud computing", *IEEE Communications Surveys and tutorials, pp 2394-187, April 2015.*

[9] Lori M. Kaufman John Harauz, "Data security in the world of cloud computing", *IEEE Computer and Reliability society, pp2456-245, JAN 15.*

[10] Indrajit Rajput, "Enhanced data security in cloud computing with third party auditor", *in proceeding of IJARCSSE, March 2013.*

[11] Sanjoli Singla and Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique", *In proceeding of IJARCET, Vol 2, Issue 7, July 2013.*

[12] Parul Mukhi and Bhawna Chauhan, "Survey on triple system security in cloud computing*", In proceeding of IJCSMC, Vol. 3, Issue. 4, April 2014.*

[13] Aparjita Sidhu and Rajiv Mahajan, "Enhancing security in cloud computing structure", *In IJRSR Vol. 5, Issue, 1, pp.128-132, January, 2014.*

[14] K. S. Wagh, Swapnil Chaudhari, and Anita Deshmukh at al., "Data Security in Cloud Computing", *In proceeding of International Journal of Current Engineering and Technology, 2014.*

[15] R. Bala Chandar, M. S. Kavitha and K. Seenivasan, "A proficient model for high end security in cloud computing", *ICTACT journal on soft computing, Vol. 04, issue: 02, Jan 2014.*

[16] M. K. Sarkar and Trijit Chatterjee, "Enhancing Data Storage Security in Cloud Computing Through Steganography", *ACEEE Int. J. on Network Security, Vol. 5, No. 1, Jan 2014.*

[17] Varsha Y. and Preeti A., "Fingerprinting Based Recursive Information Hiding Strategy in Cloud Computing Environment", *IJCSMC, Vol. 3, and Issue. 5, May 2014.*

[18] Wikipedia, "Cloud computing", *https://en.wikipedia.org/wiki/Cloud_computing#Origin_of_the_term", visited on 10/10/2015.*

[19] Muthakshi, Meyyappan and Phil, "Survey on Security Services in Cloud", *In Proceeding of NIST, Sept 2011.*

[20] Wikipedia, "Steganography", *https://en.wikipedia.org/wiki/Steganography, visited on 10/10/2015.*

[21] Wikipedia, "Advance Encryption Standars", *http://en.wikipedia.org/Advanced_Encryption_Standard.*

[22] Amazon.com, "Amazon Web Services (AWS)", *Online at hppt://aws.amazon.com, 2014.*

[23] Michael M., "Cloud Computing"*, 1st edition, pearson, 2009.*

[24] T. Pasquier, B. Shand, and J. M. Bacon, "Information flow control for a medical web," *In e-Society, IADIS, 2013.*

[25] Google, "The white paper was released in the Official Google Blog post", *Gmail: It's cooler in the cloud, 2013.*

[26] Gurpreet S., "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security",*In International Journal of Computer Applications (IJCA), Vol.67, No.19, April 2013.*

[27] Kritika S., "Hash Based Approach for Secure Image Steganography Using Canny Edge Detection Method", *IJCSC, Vol.3, No., 1 pp.155-157, June 2012.*

[28] "Steganogrphy Research Paper", *http://www.engpaper.net/steganography-research-papers-2014.htm, visited on 10/11/2015.*

[29] Github, "WiFly Library, *https://github.com/openshift,visited on 2/10/2015.*