Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 112-122
https://doi.org//10.47514/kjcs/2024.1.1.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

User Centered Data Security in Cloud Computing Using Steganography

Abdullahi Tanimu[1], Kabir Musa[2], Salisu Zubairu[3], Lugman Yusuf[4] and Yusuf Abubakar[5]
[1]Department of Computer Science, Kaduna state University
[2, 3, 5,] Department of Computer Science, Nuhu Bamalli Polytechnic, Zaria.
[4]Department of Mathematics, Kaduna state University
Abdullahitanimu358@gmail.com, musakabir16@gmail.com, salisaz@live.com, luqmanyusuf27@kasu.edu.ng, yusufabukausar@gmail.com,

Abstract

Cloud computing is one of the result of rapid growth of computing technology which has now affect the very way by which organizations and individuals uses IT resources such as application, storage, etc. by providing shared virtual versions of such resources which comes with the benefit of reducing the cost of hardware and software installation, but the concerns of organizations lies within the security and privacy of their data at rest on the cloud storage, among such concerns are the unauthorized usage by possible malicious insider within the cloud provider organisation and other cloud users. Despite the fact that service providers used many mechanisms to protect unauthorized access to data stored in their cloud storage, but there is no any mechanism to protect unauthorized access to the client's data by the cloud service administrator. In this work we show how a steganography which is a technique of concealing the existence of a data inside a cover medium can be used to improve the security of data in the cloud by using additional layer of security that is user centric. However, the application of the proposed technique is implemented using a particular case study.

Keywords: *keyword_ Cloud Computing Security, CSPs, LSB steganography, stego-image, Steganalysis.*

1. Introduction

In the current world of computing, cloud computing stands as a paradigm shift in the process of managing, distributing and storing data. Cloud computing provides online information storage, infrastructure and application as services to the client and such services are provided according to the users need (Shirole and Vishwamitra, 2021). The services are deployed and provided as different service using different deployment models. Cloud computing has three service models which are Software as a Service (SAAS) which provide services that makes the application running on the provider's server accessible to the client, Platform as a Service (PAAS) which enables the user to deploy his own implemented application unto the cloud and then Cloud Infrastructure as a Service (IAAS) which involves enabling the client to provision processing, storage, networks, and other computing resources and also opportunity for clients to deploy and run arbitrary software using any of the deployment models. These deployment models which can be community, public, private or hybrid cloud are used to define the mode of access to the cloud services. The community cloud offers services to a group of users that uses the cloud for a common purpose, the private cloud limit access to only single user which may be an individual or organization, while the public makes the cloud resources available to general public, therefore anybody can access services provided by the public cloud and the hybrid cloud composed the features of both the public and private clouds (Rajeswari, 2019). Obviously,

Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 112-122
https://doi.org//10.47514/kjcs/2024.1.1.009
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

cloud computing, offer virtual computing services and resources to a large number of users. One of these services that are provided is the cloud storage which allows users to store their data using the cloud storage infrastructure. Despite the obvious benefit of information availability, this use of cloud present security concerns (such as malicious behaviour of insiders, responsibility ambiguity, cloud service abuses, etc.) for organizations' or individuals' data stored over the cloud as the security of the data is concentrated with the cloud provider or is shared between the provider and the client. These security concerns present issues relating to privacy and trust for data stored over the cloud storage and is a problem that needs to be solved so that cloud can be trusted by every individual and organisations. Digital Steganography which is the act of concealing the existence of data using a cover medium (Singh et al., 2019) (image, video, or audio) can be useful in this regard as the existence of the actual information stored can be hidden even to the cloud service provider at the user level so that the existence of the actual data stored cannot be known (Abdallah and Rahmah, 2016). Therefore this work involve a study on cloud computing security, relevant literatures will be reviewed and we will also study steganography and more specifically LSB steganography in order to find how it can be used to ensure the security of information that is to be uploaded over the cloud storage which will give the opportunity of coming up with a method to provide the security of information stored in cloud storage using steganography.

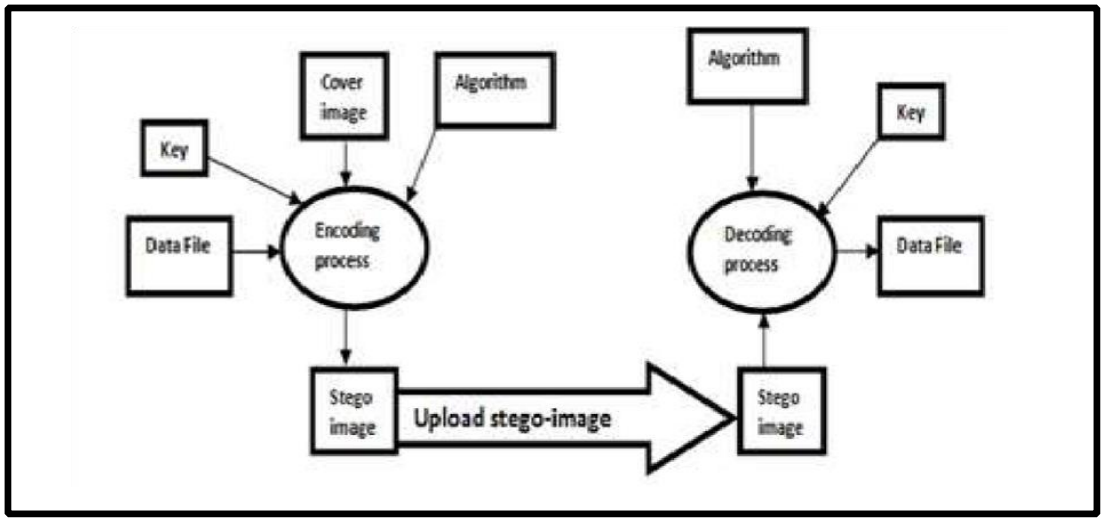

Figure 1: Architecture of the Steganography System (Source: Champkamamala et al., 2014)

2. Related Works

Different literatures addressed the security issues of cloud computing by suggesting methods to help guarantee the security of data stored in the cloud. Shirole and Vishwamitra (2021) proposed a method of data security in cloud computing using encryption, the method encode the data which is then uploaded to the cloud. The data is encrypted in rounds with an encryption method to follow in each round, data is used as input to the rounds, using three steps of transport sub bytes, row transit, and round key. The approach is not simple in its approach and also from security point of view it is feasibly questionable as extensive use of encryption algorithm is done but no care has been taken to secure the key used for encryption.

Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 112-122
https://doi.org//10.47514/kjcs/2024.1.1.009
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

Ibitayo et al., 2022 proposed a scheme that uses both cryptography and steganography, they apply steganography on the encrypted file uploaded to the cloud. They used symmetric algorithm for the encryption of the file uploaded to the cloud. The method can provide security of data stored in the cloud, but however, the method adopted still maintain the cloud provider in its implementation.

Ajala et al, 2019 proposed a steganography scheme in which a cloud server system randomly produce access keys after a record is made by the user concerning a specific information. In the process, the proprietor swiftly encode the records concealing data into a picture that is later split and stored in the cloud.

Singla and Bala (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.

El-latif et al. (2018) discussed the necessity 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.

Ravi and Ashish (2013), in their Paper on "Data Security for Cloud while using Third Party Auditor", this paper uses the services of a third party auditor for checking cloud service's provider reliability. Also it verifies that the data is intact and is responsible for its accountability. In short it deals with the problem of data privacy and its integrity.

Bala et al., 2014 in their paper, "A proficient model for high end security in cloud computing", this paper presents a protocol that uses the services of a third party auditor not only to verify the integrity of data stored at remote servers but also in retrieving the data in intact form. The main advantage of this scheme is the use of digital signature to assure the integrity of data locally. However, the overall process is quite complex as the keys and data are also encrypted and decrypted respectively.

Al-khanjari and Alani, 2014 proposed a steganography scheme architectural model to protect data in cloud. Security is one of the important issues discussed and resolved in this paper using protected access control technique which can prevent security problems. Authors proposed steganography scheme that uses text properties to hide the data, text properties includes font, font metrics, font styles, color and RGB values, and the x, y location to display data. This steganography support cloud computing to provides security from unauthorized access. The architecture contains 3 layers physical layer, data layer, security layer (Pardede et al., 2014). Security layer hide the data through security pipeline channel.

Brohi et al., 2014 provide a solution for data privacy issues in some organisations that uses personal data of their clients. The authors implement the holomorphic version of RSA algorithm to encrypt, decrypt and process the encrypted data on cloud. Encrypted data is usually uploaded to the cloud. This technique not allows the cloud to

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

process the data on the cloud when it is encrypted and the server required that clients should provide a private key before they can be able to decrypt the encrypted data and use. "Cloud computing security using encryption technique", deal with the issue of data security during transmission of data. The main concern here is to encrypt the data so that confidentiality and privacy can be achieved. The algorithm used here is Rijndael Encryption Algorithm along with EAP- CHAP

Varsha (2013). Paper on "Cloud Computing Security and encryption", the author has tried to attract analyst attention towards the problem of data security and as firmly believe that data encryption can help to solve this issue. The author has provided a list of various encryption techniques such as RSA, DES. Most of the literatures above, provide a security mechanism that involved the cloud service provider in its implementation. There is need for a security model that enable the client to protect his data at his level in addition to the security mechanism provided by the CSPs.

3. Methodology

The proposed technique allows clients to protect their own data which are to be uploaded unto the cloud by using a steganography application at their level. **Figure 2** shows the architecture of the proposed technique. It can be seen as a client-server system which involves the following components:

- **Client** who select a cover image, data file, algorithm and password or a key.
- **Computing device** (smart phone, laptop, desktop, etc) on which the steganography application is running.
- **A steganography application** that is used for embedding secret data inside a cover image and extracting the embedded data from the cover image and in our proposed model, this steganography application is only accessible to the client.
- **Cloud computing provider** providing various cloud computing services.

In the proposed technique, the user is responsible for using steganography application on any computing device to generate stego-image to be stored on the cloud server. When the image is retrieved from the cloud, the user also uses steganography application to extract the data from the retrieved stego-image.

Our proposed technique uses 24-bit images to embed data. We used 24-bits image because it can display more than 16000 different combinations that can easily hide data in a way that it will be hard to detect any difference between the modified image and the original image. The application is deployed and used on the user's side and therefore only the user knows about the application and the key that was used in embedding and therefore there is no need for exchange of key between the cloud user and the cloud service provider.

The digital images are represented using an array of pixels. These pixels represent the intensities of three colors; red, green and blue (also known as RGB). In RGB model, a value of each color describes a pixel. In our case we are using LSB approach for hiding information into an image. Therefore we show how the data embedding of using LSB is performed. Assuming that the user wants to embed letter "B" into a 24-bits image and the binary value of "B" is 10000100. In 24-bit image each pixel has eight bits for each color in RGB model. The user needs to change the LSB that require only 3 pixels for hiding 8 bits letter "B", the original 3 pixels are represented in the table 1 below:

Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 112-122
https://doi.org//10.47514/kjcs/2024.1.1.009
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

Table 1. 24-bits word

	RED	GREEN	BLUE
Pixel 0	00100111	11101001	11001000
Pixel 1	0010011	11001000	11101001
Pixel 2	11001000	00100111	11101001

Table 2. 24-bits word after inserting the letter B

	RED	GREEN	BLUE
Pixel 0	00100111	11101000	11001000
Pixel 1	00100110	11001000	11101001
Pixel 2	11001000	00100110	11101001

Each row of the table represents each pixel and each column represents RGB value for each pixel. After embedding the final value of "B" into the three pixels starting from the top left byte in the table and going to the right end. Following the same sequence for each row will generate result generated in the Table 2.

The most important feature of the proposed technique is that, the additional security layer that is added is only the user knows about it, the cloud provider will only receive a stego-image uploaded by the user and also add the cloud security mechanism in addition to the user steganography and the user can access and use his data from any of the computing device that he used to connect to the cloud. It will add an additional level of security that only the client knows of it, as in figure 2 below, the steganography system used is only accessible to the user who will upload or retrieve data from the client and the service provider and other cloud cannot access the steganography application thereby improving the security of data both in transit and at rest.

Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 112-122
https://doi.org//10.47514/kjcs/2024.1.1.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

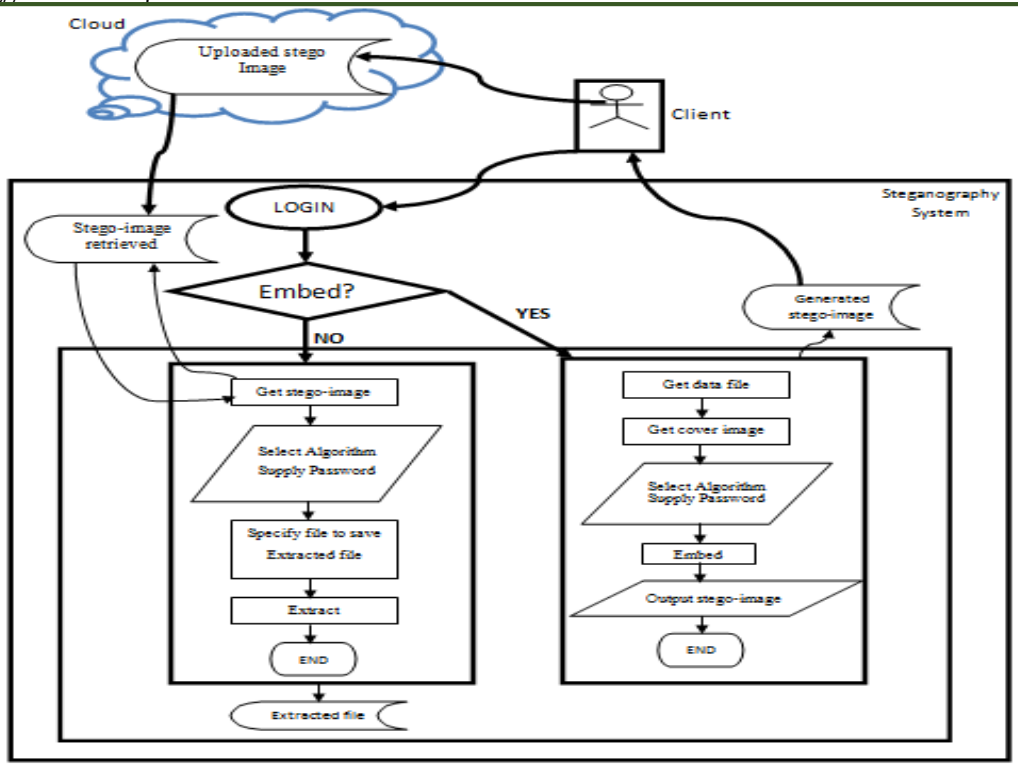

Figure 2: Proposed system Architecture

Uploading Process

To upload a data unto the cloud storage, there is need to firstly subscribe to cloud storage infrastructure of any of the service providers. A steganography system is then used to conceal the existence of the data to be uploaded as follows:

- User first login to the steganography system at the client site by supplying correct login credentials
- The client can then use the steganography system accessed to hide any file containing the data needs to be uploaded to the cloud by:
- Selecting the file containing the data he wants to upload to the cloud.
- The user then Select the cover image to use in hiding the data to be uploaded unto the cloud storage.
- Supply password to use in hiding the data
- Select algorithm to use.
- Select the file to store the stego image.
- Click on embed button to hide the selected file in the selected image.

After successfully hiding the file in the cover image, another image which is stego image will be achieved. The user can then upload this stego image unto the cloud.

Retrieval Process

The user will first retrieve the stego-image file uploaded unto the cloud, he can then use the steganography system to extract the data hidden in the retrieved stego-image as follows:

Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 112-122
https://doi.org//10.47514/kjcs/2024.1.1.009
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

- The user selects the extract option and the extract interface will appear.
- Browse the stego-image retrieved from the cloud storage
- Select the password and the algorithm used during embedding.
- Specify the file to save the extracted file containing the hidden data.
- Click on extract to extract the hidden file.

The above method, introduced a security level that is only known by the cloud user as the actual data is only known by the client.

To study how the proposed method work, we used a steganography application that implemented two steganography algorithms (blind hide and hide seek), we then used the implementation to hide data in some images, and a questionnaire is then used to find whether cloud users can identify any difference between the original image and the stego-image.

Therefore, twenty individuals (ten constant web/cloud users, ten IT students/professionals) were used to identify the differences between original cover images and the stego-images generated by the steganography methods used.

4. Result and Discussions

A steganography scheme is said to be secured only if a Human Visual system (HVS) cannot understand the presence of hidden data in medium embedded with data. Therefore, to study the strength of the proposed method, we implemented a steganography system using Java and then use the steganography system to generate stego images that are to be uploaded to the cloud (see figures 3 to 5). We then presented these generated stego images and the original image to some cloud users for them to perceive any visible difference between the original cover image and the stego-image. The result of the responses indicated that none of the respondent is able to identify any difference between the images, see table 3 and 4.

Figure 3**:** original image

Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 112-122
https://doi.org//10.47514/kjcs/2024.1.1.009

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

Figure4: image embedded with data using blind hide algorithm

Figure 5: image embedded with data using hide seek algorithm

Table 3. Result for measuring the imperceptibility of an image embedded with data using blind hide algorithm

Questions/ responses	Agree	Strongly Agree	Natural	Disagree	Strongly disagree
Q3	9	6	2	0	0
Q4	7	7	3	0	0

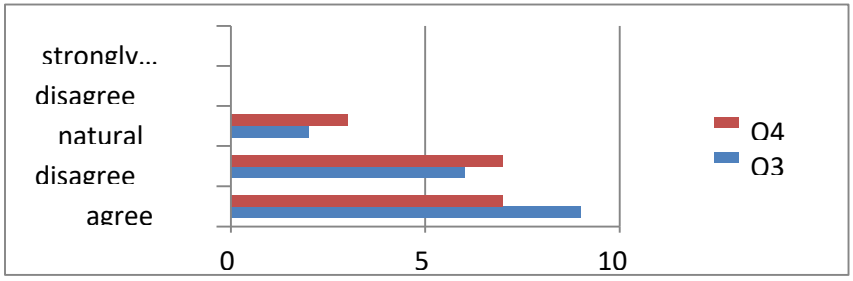

Figure 6**:** Result of measuring the imperceptibility of image embedded with data using blind hide algorithm of LSB

Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 112-122
https://doi.org//10.47514/kjcs/2024.1.1.009
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

Table 4. Result for measuring the imperceptibility of an image embedded with data using hide seek algorithm

Questions/ responses	Agree	Strongly Agree	Natural	Disagree	Strongly disagree
Q6	7	9	1	0	0
Q7	10	6	1	0	0

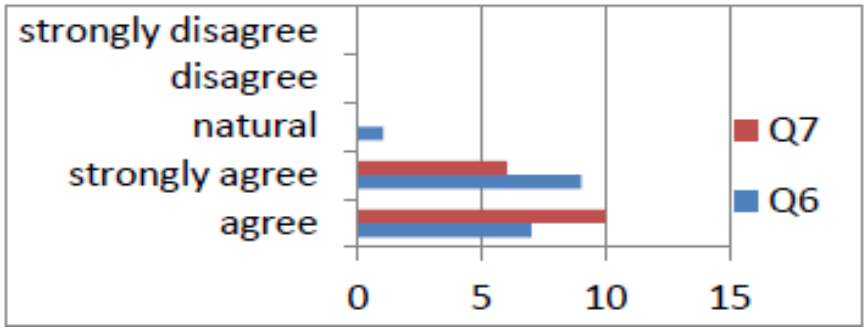

Figure 7**:** Figure: result of measuring the imperceptibility of image embedded with data using hide seek algorithm of LSB

The general results of this survey indicates that the method proposed recorded a high level of imperceptibility to visual steganalysis as the human visual system (HVS) cannot detect the difference between the real copy of the image and the image containing the secret information to be uploaded unto the cloud storage. Another important security issue addressed by this work is the possibility of malicious insider within the CSPs organisation to have access to the hidden data, the proposed technique uses the steganography at user level, in such a way that only the client that uploaded the data have access to the steganography application used in embedding the data, the client also is the only user with the knowledge of the algorithm used in embedding the data. Another strength of the proposed technique is that, the cover image will not be available to other cloud users and therefore, malicious users cannot have it easily possible to perform statistical comparison of the stego-image and the original image.

5. Conclusion

In this paper, we proposed a model that uses steganography to conceal the data that is to be uploaded unto the cloud. We have demonstrated how the proposed method can be used to hide information that is to be uploaded to the cloud and the result of our experiment with cloud users indicated that the stego-images generated by the steganography system used in this work are protected from visual steganalysis as the human eyes cannot be able to identify the existence of any hidden information with the stego-images generated and with this, the secret data embedded in the stego-image cannot be known by the cloud users (administrators and clients). Statistical comparison of the original and stego-image is also not possible at the cloud, this is because, in our proposed technique, what will only be saved on the cloud is stego-image and therefore attacker cannot be able to do such comparison as there is no original copy of the image that can be used to find whether that image is containing any hidden information what he can only obtained is the statistical properties of only stego-image and that is why we are recommending that in using steganography to hide the existence of data we should not use widely available images on the internet. Future work

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

should focus on how to improve the data security at user level using algorithm that can on themselves protect the particular stego-images against any kind of steganalysis.

Reference

Abdullah, W. F. and Rahma A. S. (2016). A Review on Steganography Techniques. American Scientific Research Journal for Engineering, Technology, and Sciences, 24(1), 131-150. http://asrjetsjournal.org.

Ajala, J. A., Singh, S. & Mukherjee S. (2019). International Conference on Computational Intelligence and knowledge Econoy (ICCIKE), Dubai, UAE, 2019.

Al-khanjari, Z. and Alani, A. (2014) Developing interoperable cloud computing Services. The European Interdisciplinary Forum 2014 (EIF 2014), Vilnius, 18-19 June 2014, 341-350.

Aparjita, S. & Rajiv, V. (2014) "Enhancing security in cloud computing structure by hybrid encryption", *International Journal of Recent Scientific Research* Vol. 5, Issue, 1, pp.128-132, January, 2014.

Bala, R. C., Kavitha, M. S. & Seenivasan, K. (2014) A proficient model for high end security in cloud computing. *ICTACT Journal of Soft Computing.* January, 2014, 4(2), 2229-6956. http://doi.org/10.21917/ijsc.2014.0100.

Brohi, S., Bamiah, M., Chupra, S., & Manan, J. (2014). Design and Implementation of a Preserved Off-Premises Cloud Storage. *Journal of Computer Science,* 10, 210-223. http://dx.doi.org/10.3844/jcss. 2014.210.223.

Champakamala, B. S., Padmini, K., Professors, R. D. K. A. & Bosco, D. (2014) "Least Significant Bit algorithm for image Steganography Overview Of Steganography", *International Journal Of Advanced Computer Technology*, Vol. 3 No. 4 p. 5

Denis, R. & Madhula, P. (2020). Evolutionary Computing Assisted Visual Imperceptible Hybrid Cryptography and Steganography Model for Secure Data Communication over Cloud Environment. International Journal of Computer Network and Applications, 7(6), 208-230. https://doi.org/10.22247/ijcna/2020/205321.

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

Hassan, Qusay (2011). "Demystifying Cloud Computing"*(PDF). The Journal of Defense Software* Engineering. Cross Talk. 2011 (Jan/Feb): 16–21. Retrieved 11 August 2018.

Ibitayo, F. B., Abimbola O. R. & Oyeladun, M. B. (2022). Securing Cloud Computing with Cryptography and Steganography. International Journal of Science and Engineering Applications, 11(6), 76-88. https://doi.org/10.7753/IJSEA1106.1002.

Ibrahim, D. S. (2019). Enhancing Cloud Computing Using Cryptography and Steganography. International Journal of Information Technology, 9(2), 191-224.

Jathanna, R. and Jagli, D. (2017). Cloud Computing and Security Issues. International Journal of Engineering Research and Application. 7(6) 31-38

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.com.ng

Kumar, N. K., and Naresh, M. (2017) Security threats in cloud computing. *International Conference on Emerging Trends in Engineering, Science and Management.* **2017**, p983-992.

Mell, P. & Grance, T. (2011) The NIST Definition of cloud Computing, NIST Special publication, US Department of Commerce.

Rajeswari M. N. (2019). Overview of cloud computing and its types. Journal of Emerging Technology and Innovative Research (JETIR), 6(3), 61-67. https: www.researchgate.net/publication/354683300

Ravi, K. S. and Ashish B. (2013) Data Security for Cloud while using Third Party Auditor. *International Journal of Computer Application (0975-8887) 70(16).*

Singh S. k., Manjihi P. K. & Tiwari R. K. (2019). Cloud computing security using steganography. Journal of Emerging Technologies and Innovative Research. 6(6), 2349-5162.

Singla, S. & Bala, A. (2018), "A Review: Cryptography and Steganography Algorithm for Cloud Computing". Second International Conference Invention Communication and Computing Technology, no. Icicct, pp. 953–957, 2018.

Shirole, B. S., Vishwamitra L. K. (2021). Data Security in Cloud Computing: a Novel approach and objectives. Journal of Tianjin University of Science and Technology, 54(9), 140-152. https://doi.org/10.17605/OSF.IO/F8TPQ.

Varsha, A. (2013). Cloud Computing Security and encryption. IJMC, 3(5).

Sahu, D., Sharma, S., Dubey, V. and Tripathi, A. (2012) Cloud Computing in Mobile Applications. *International Journal of Scientific and Research Publications*, **2**, 1-9. Virtualization Overview. White Paper. Vmware. Retrieved April 6, 2018, available at:http://www.vmware.com/pdf/virtualization.pdf Web Search for A Planet: The Google Cluster Architecture. Retrieved April 6, 2022, available at: http://labs.google.com/papers/googlecluster-ieee.pdf