Implementation of an Improved Multi-Channel Security in Cloud Computing Using Image Steganography and RSA Algorithm

Ismail Abdulkarim Adamu [1], Souley Boukari [2], Hajara Musa [3], Fatima Umar Zambuk[4]

[1]*(Department of Computer Science, Gombe State Polytechnic, Bajoga, Gombe Nigeria)*
[2]*(Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi, Nigeria)*
[3]*(Department of Mathematics, Gombe State University, Gombe Nigeria)*
[4]*(Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi, Nigeria)*
Corresponding Author: Ismail Abdulkarim Adamu

Abstract: *The increase use of cloud computing infrastructure has led to a security consciousness by users and cloud service providers to protect data available in the cloud from illegal users. Even though, different techniques have been proposed by different researchers, yet, more techniques are still proposed all in the quest to achieve better and flexible security techniques that will utilize less resource and minimize cost, because user pay as they go in the cloud. In this paper we proposed an improved multi-channel security technique in the cloud using image steganography and RSA algorithm. The proposed method was used to conceal the existence of data communication using the image steganography and protect the concealed data using RSA encryption algorithm in order to prevent illegal access. Different data set such as text, image, audio and video were used to evaluate the system. It is shown in the analysis that text data utilizes less processing time, memory storage and processing power followed by image, video and audio data set. Except, for processing power where all the data set utilizes the same network bandwidth. Also, the technique provides a strong security measure to prevent illegal access to stored data in the cloud.*

Keywords: *Cloud computing, Image steganography, RSA algorithm*

Date of Submission: 20-12-2018 Date of acceptance: 06-01-2019

I. Introduction

Cloud computing provides platform that allows users to upload their data and have access to other available resources such as memory storage, network server, operating system etc. which reduces cost for the users [1]. The availability of these resources in the cloud makes start up individual, companies and organizations to access and use such resources automatically by paying for the services rather than buying and maintaining it themselves [2]. Once, user data is uploaded to the cloud, the control of the data becomes under the control of the cloud service providers. This has posed so much concern to the cloud users because the security and privacy of their data is at stake [3]. Since the user will not know who is accessing their data, the location of the data and the types of data stored with their data which may lead to illegal access or damage of the data [4]. In order to guarantee the security and privacy of user data in the cloud environment different security measures have been considered by different researchers [5]. Among such techniques considered are cryptography and steganography. Cryptography converts the data into non meaningful format to the unauthorized user in trying to convey the data to the intended users [6]. In the same vein, steganography is used to conceal the existence of the communication of user data in the cloud. Steganography uses text, image, audio and video content as a cover for concealing and transferring user data in the cloud [7]. Due to the increase threat posed by intruders in the cloud, more research are ongoing in order to come up with a better security technique that will secure user data with minimal resources in the cloud. In this paper we implement an improved multi-channel approach to secure data in the cloud using the combination of image steganography and RSA algorithm.

II. Image Steganography

Image steganography is a method used to conceal the existence of communication from unauthorized user in an image cover (Tiwari & Shandilya, 2010). In image steganography the information to be communicated are hidden within the pixel intensity of the image. In general term the information are hidden within a cover image in order to generate a stegano image which will be communicated to the intended users [9]. To successfully conceal data using image steganography there are terms used as indicated in [10] as follows:

i. **Cover image:** this is the carrier of the message used to successfully convey the message without perception of the unauthorized user.
ii. **Stego image:** this is the concealed message to be communicated with to the intended user.
iii. **Message:** the message to be concealed in order to be communicated with.
iv. **Stego Key:** it is the secret key used for concealing and extracting the concealed message being communicated.

Figure1 describes the working principles of image steganography.

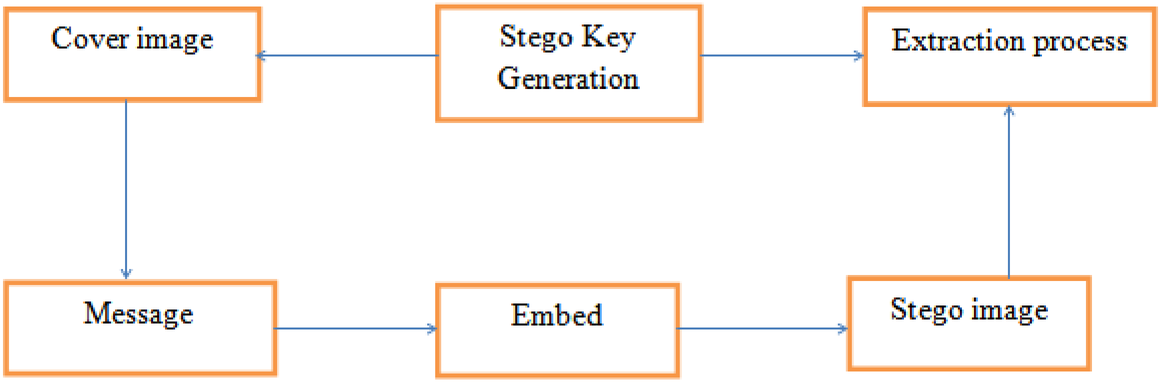

Figure1: Working principles of Image steganography

III. Riverst Shamir Adleman (RSA) Encryption Algorithm

RSA algorithm is one of the asymmetric encryption algorithms that use two keys such as public and private keys for encryption and decryption. The public key is used for encryption and shared among all users whereas the private key is known to only the intended user for decrypting the content that was encrypted [11].
The working procedures of RSA encryption algorithm is described as follows:
Step1: Select two large prime integers denoted as p and q
Step2: compute n = p * q. Where n represent the product of the large integers obtained.
Step3: n = (p - 1) * (q - 1)
Step4: The encryption key is selected randomly where $1<e< \varphi (n), gcd (e,\varphi(n)) =1$
Step5: To obtain the decryption d the following is used:De = 1mod φ *(n) and 0* ≤ d ≤ n
Step6: public key PU = e, n.
Step7: private key PR = d, n

IV. Literature Review

Considering the fact that capacity fitness is an important factor in embedding secret text in text steganography, [12], conducted performance analysis of changing in alphabet patterns (CALP), Vertical straight line (VERT) and quadruple categorization (QUAD) considering their embedding ratio and saving space ratio. Their analysis proved vertical straight line (VERT) to have a better performance in embedding ratio and saving space ratio. The exponential growth of information communication over the internet is posing a serious sinister to the internet user. To overcome such degree of threat, a dual security technique was proposed in [13] to provide a strong secure means of conveying secret information over the internet. The proposed technique hides data in three phases; first by encrypting the data using vigenere cipher, secondly by applying white space text steganography technique on the image cover used to concealed the existence of the secret message and thirdly by hiding the cover text in image using LSB steganography technique. [14], proposed a multiple layer security technique using modified AES_MPK and image steganography in order to secure data communication. The proposed technique works by first encrypting the secret data using the modified AES_MPK algorithm and then the encrypted secret message is concealed in gray images using PVD_MPK and MSLDIP_MPK methods. The proposed algorithm provides a strong secured communication and increase PSNR compared to other proposed algorithm. Double layer of security mechanism to secure communication was proposed combining image steganography and cryptography in [15]. In their proposed model, RSA was used for encrypting and decrypting the secret message and Diffie-Hellman Algorithm used to select the pixel of the image with which to embed the secret messages. The proposed model produced a good quality image after inserting a high capacity of secret message. The increased use of the internet for data communication has made it necessary for users to secure their data against intruders attack while transferring the data from one point to the other. [16], proposed an encryption technique to provide secure data transfer over a workgroup communication system using image LSB steganography and RSA cryptography method. The proposed method send a notification signal to the admin whenever a three (3) wrong password attempt was made to detect a guilty user for necessary action by the admin. However, with all this solution provided by different researchers, more research are ongoing in a quest for getting a solution that will minimize cost and consume less resources in the cloud.

V. Methodology

In this research we proposed an improved multi-channel approach for communicating secret messages from sender to the receiver in the cloud. The proposed technique worked by encrypting the intended secret message to be communicated using RSA encryption algorithm. After which, the encrypted message is then concealed using image steganography to prevent unauthorized user from perceiving the existence of the communication.

Working principles of the proposed algorithm

1. Start
2. Create secret message
3. Encrypt message using RSA public key
4. Conceal message using image steganography
5. Upload concealed message
6. End

Flowchart of the proposed system

Figure2 is the flowchart of the proposed system. It described how the proposed system executes from start to finish.

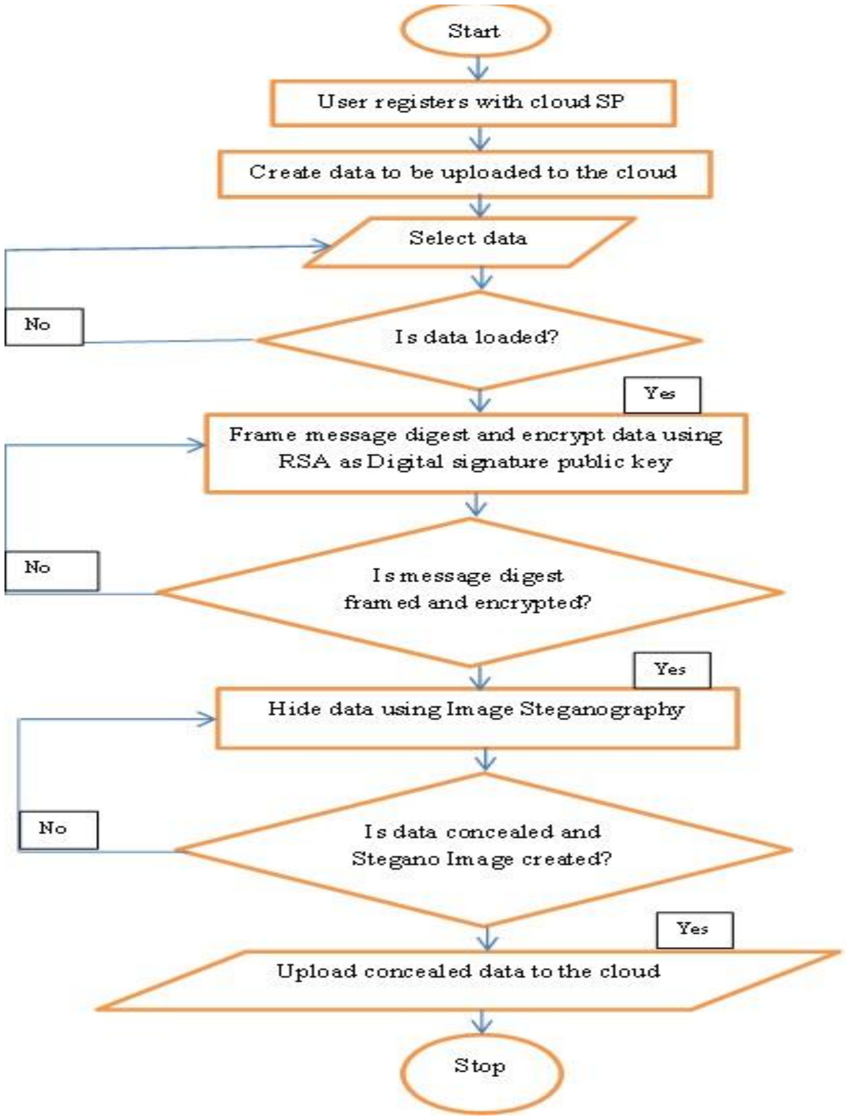
Start
User registers with cloud SP
Create data to be uploaded to the cloud
Select data
No
Is data loaded?
Yes
Frame message digest and encrypt data using RSA as Digital signature public key
No
Is message digest framed and encrypted?
Yes
Hide data using Image Steganography
No
Is data concealed and Stegano Image created?
Yes
Upload concealed data to the cloud
Stop

Figure2: Flowchart of the proposed system

VI. Result and Discussion

It is obvious that the increase patronage of cloud facility is for the fact that, cloud offer unlimited storage capacity and network bandwidth to be utilized by the user. Furthermore, processing speed and system power consumed are also vital in vying for cloud computing. As a result, in this proposed work we improve and evaluate the performance of image steganography and RSA algorithm considering the processing time, Storage memory, processing power and bandwidth consumed. To ascertain the desired result, Java programming language was used to develop and simulate the behavior of the proposed system in the cloud. The data used for evaluation are text, image, audio and video data types. This is as the result of the frequent used of these data in the cloud. The results obtained are shown and discussed as follows:

Processing Time

Table1. Processing time consumed by the proposed system using different date types on different data size.

S/N	Data size	Text (Sec)	Image (Sec)	Audio (Sec)	Video (Sec)
1	1mb	6.407	6.8	7.603	8.83
2	2mb	7.334	10.159	9.59	10.245
3	3mb	7.918	10.403	11.345	12.158
4	4mb	7.302	11.075	12.443	10.673
5	5mb	7.512	14.386	12.32	12.659
6	6mb	14.662	14.836	14.202	15.211
7	7mb	6.856	15.655	14.848	15.933
8	8mb	5.776	15.662	23.489	15.709
	Average	**7.971 Sec**	**12.372 Sec**	**13.23 Sec**	**12.677 Sec**

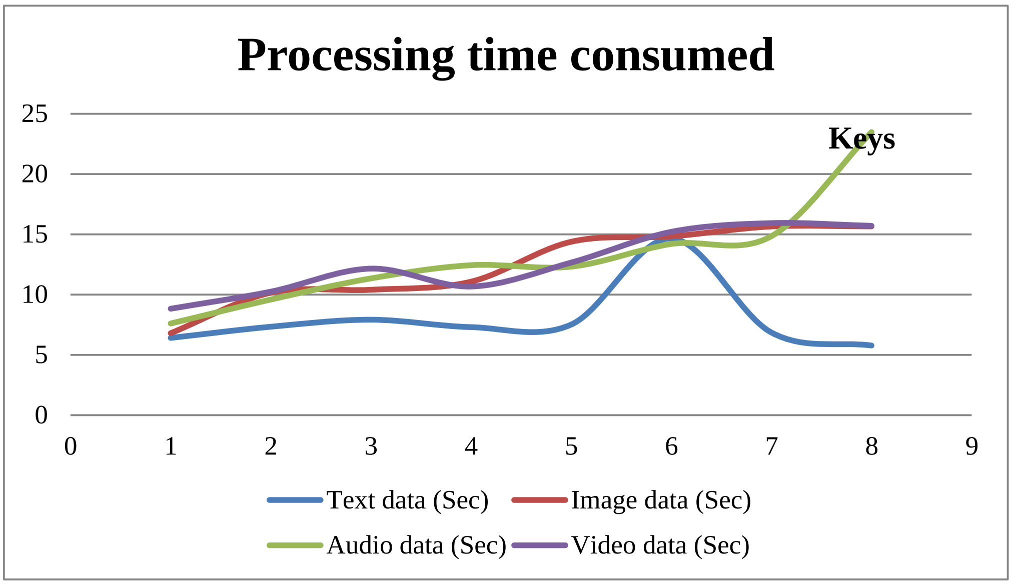

Figure3. Processing Time Consumed By the Different Data Types on the Proposed System

The processing time consumed by the different data types on different data size is shown in figure3. The result shows that Audio data type takes more time to process data on the proposed system with an average processing time of 13.23 seconds followed by Video with 12.677 seconds, Image with 12.372 seconds and Text data type with 7.971 seconds.

Memory Storage Consumed

Table2. Memory storage consumed by the proposed system using different date types on different data size.

S/N	Data size	Text (kb)	Image (kb)	Audio (kb)	Video (kb)
1	1mb	41.224	48.22	42.258	58.052
2	2mb	33.446	48.327	46.806	37.934
3	3mb	38.941	93.479	115.334	61.722
4	4mb	67.564	58.419	59.5	72.201
5	5mb	60.650	71.933	87.206	104.282
6	6mb	65.477	81.968	89.871	108.915
7	7mb	112.023	100.391	91.021	154.444
8	8mb	74.626	186.053	147.969	152.981
	Average	**61.744 kb**	**86.099 kb**	**84.995 kb**	**93.816 kb**

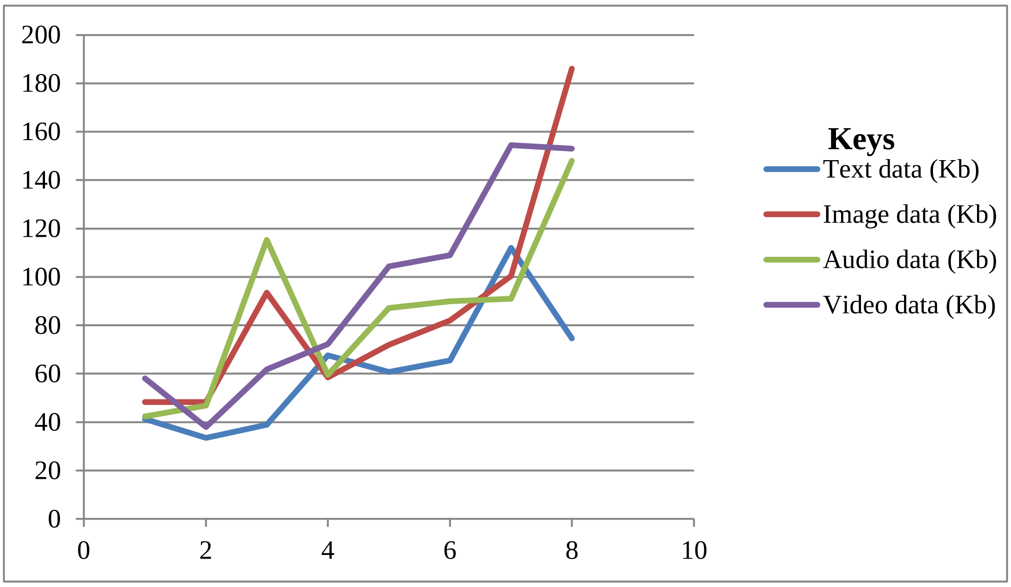

Figure4. Storage Memory Consumed By Different Data Types on the Proposed System

Memory storage consumed by the different data types on different data size is shown in figure4. The result shows that Video data utilizes more memory storage to process data on the proposed system with an average memory size of 93.816 kb followed by Image with 86.099 kb, Audio with 84.995 kb and Text data type with 61.744 kb.

Processing Power Utilization

Table3. Processing power utilization Consumed by the proposed system using different date types on different data size.

S/N	Data size	Text (kwh)	Image (kwh)	Audio (kwh)	Video (kwh)
1	1mb	7.688	8.16	9.124	10.596
2	2mb	8.801	12.191	11.508	12.294
3	3mb	9.502	12.484	13.614	14.589
4	4mb	8.762	13.29	14.932	12.808
5	5mb	9.014	17.263	14.784	15.191
6	6mb	17.594	17.803	17.042	18.253
7	7mb	8.227	18.786	17.818	19.119
8	8mb	6.931	18.794	28.187	18.851
	Average	**9.565 kwh**	**14.846 kwh**	**15.876 kwh**	**15.213 kwh**

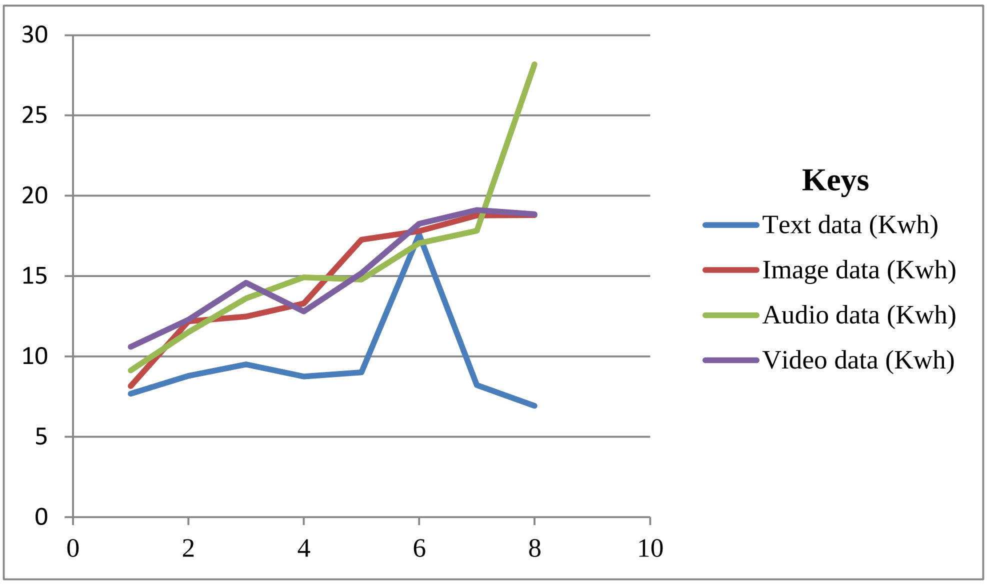

Figure5. System Processing Power Consumed by Different Data Types on the Proposed System

The system processing power consumed by the different data types on different data size is displayed in figure5. The result shows that Audio data utilizes more system processing power to process data on the proposed system with an average processing power of 15.876 kwh followed by Video with 15.213 kwh, Image with 14.846 kwh and Text data type with 9.565 kwh.

Bandwidth Utilization

Table4: Bandwidth utilization by the proposed system using different date types on different data size.

S/N	Data size	Text (kbs)	Image (kbs)	Audio (kbs)	Video (kbs)
1	1mb	1	1	1	1
2	2mb	2	2	2	2
3	3mb	3	3	3	3
4	4mb	4	4	4	4
5	5mb	5	5	5	5
6	6mb	6	6	6	6
7	7mb	7	7	7	7
8	8mb	8	8	8	8
	Average	**4.5 kbs**	**4.5 kbs**	**4.5 kbs**	**4.5 kbs**

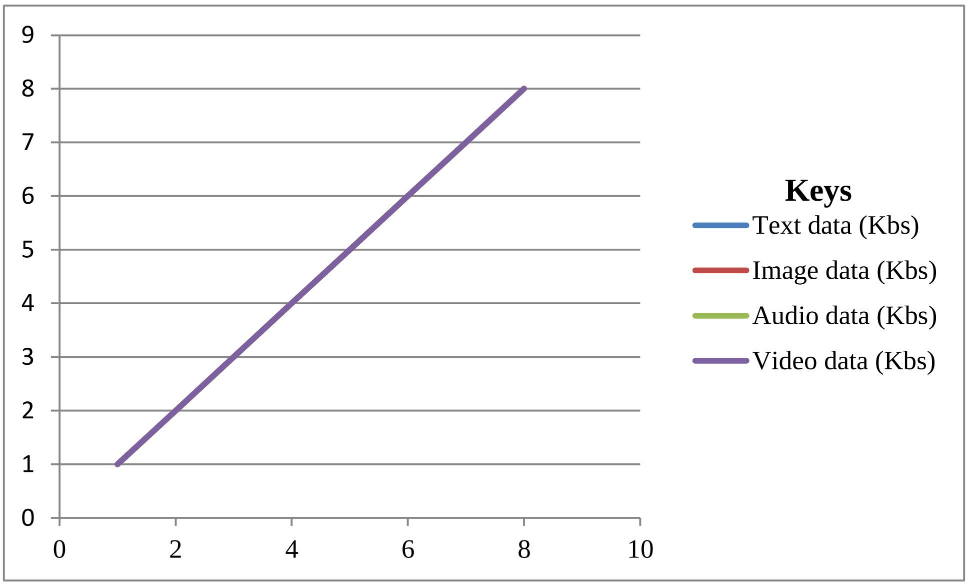

Figure6. System Bandwidth Consumed by Different Data Types on the Proposed System

The system bandwidth utilized by the different data types on different data size is displayed in figure6. The result shows that all the data types utilized the same bandwidth when processing the different data types on the proposed system with an average system bandwidth of 4.5 kbs.

VII. Conclusion

Cloud computing is attracting serious security attention in recent times due to increase of user and cybercrime related activities. Every day, new security techniques are proposed by researchers in order to overcome the security threat posed by intruders. In this paper, we proposed and improved multi-channel security algorithm using image steganography and RSA algorithm. Text, image, audio and video data set were used to evaluate the performance of the system. The result of the analysis shows that text data set consumed less processing time, storage memory and power followed by Image, video and audio data set. Except, for system bandwidth where all data set consumed the same set of bandwidth. The proposed technique provides a strong security measure in securing stored data in the cloud. In the future, we hope to evaluate the performance of the system against other system proposed by other researchers.

References

[1]. L Yuhong, S Yan, R Jungwoo, R Syed, and V V athanasios, A survey of security and privacy challenge in cloud computing: Solutions and Future Directions, *Journal of Computing Science and Engineering, 9(3),* 2015, 119-133.

[2]. B H Bhavani, and H S Guruprassad, Resource provisioning techniques in coud somputing environment: A survey, *International Journal in Computer Science and Communication Technology, 3(3),* 2014, 395-401.

[3]. Deepika, and K Gurjeet, (2016). Review Paper on Enhancing Data security for Cloud Environment Cryptography and Technique, *International Journal of Engineering Applied Sciences and Technology,* 2(1), 2016, 44-48.

[4]. J D Bokefedo, S A Ubale, and S V Pingale, Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model, *International Journal of Computer Applications*, *118(12)*, 2015, 46-52.

[5]. R Patel Palak, and P Yask, Survey on Different Methods of ImageSteganography, *International Journal of Innovative Research in Computer and Communication Engineering, 2(12),* 2014, 7614-7618.

[6]. Sharma, H Arya Mithlesh, and G Dinesh, Secure Image Hiding Algorithm using Cryptography and Steganography, *Journal of Computer Engineering, 13(5),* 2013, 01-06.

[7]. B Sneha, and B Gunjan Data Encryption by Image Steganography, *International Journal of Information and Computation Technology*, *4*, 2014, 453-458.

[8]. T Namita, and S Madhu, Evaluation of Various LSB based Methods of Image Steganography on GIF File Format, *International Journal of Computer Applications*, *6(2)*, 2010, 0975 – 8887.

[9]. H Mehdi, and H Mureed, A Survey of Image Steganography Techniques, *International Journal of Advanced Science and Technology, 54*, 2013 1-12.

[10]. K G Aparna, A solution to coud Security:Image steganography, *International Journal of Multidisplinary Research, 2(2),* 2016, 83-90.

[11]. A Marwa Ali, O Olayemi, H Keito, and T Peka, Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption, *Journal of Information Security, 9*, 2018, 168-176.

[12]. Baharudin, D Roshidi and I Mohd Rushdi, Capacity Performance of Steganography Method in Text Based Domain, *Journal of Engineering and Applied Sciences, 10(3),* 2015, 1345-1351.

[13]. S Priti, R Sarvesh, K Saurab, A Shafaq, and Y, Rohit, Hiding Encrypted Text Using Text and Image Steganography: A Dual Steganographic Technique, *International Journal Of Electrical, Electronics And Data Communication*, *5(7)*, 2017, 54-57.

[14]. E Saleh Marwa, A Aly Abdelmgeid, and A Omara, Fatima, Data Security Using Cryptography and Steganography Techniques, *International Journal of Advanced Computer Science and Applications*, *7(6),* 2016, 390-397.

[15]. S Siti Dhalila Mohd, A Hamid Nazirah, G Fatimah., M Roslinda, M Mustafa, and A Pang Kok Secure Image Steganography Using Encryption Algorithm, *Annual Int'l Conference on Intelligent Computing, Computer Science & Information Systems*, *pattaya thailand*, 2016, 43-46.

[16]. M Thakur Grjashanka, S Pratima, B Roshini, and R Mohd Jabeed, An Implementation of Steganography Technique to Provide Better Security in Workgroup Communication, *International Journal of Innovative Research in Science, Engineering and Technology*, *7(3),* 2018, 2309-2316.

Ismail Abdulkarim Adamu. " Implementation of an Improved Multi-Channel Security in Cloud Computing Using Image Steganography and RSA Algorithm. "IOSR Journal of Computer Engineering (IOSR-JCE) 20.6 (2018): 33-39.