University of Thi-Qar Journal Of Science (UTsci)
Website: jsci.utq.edu.iq **Email: jsci@utq.edu.iq**
Volume 7, Number 1, June 2019

A Review of Various Steganography Techniques in Cloud Computing

[1]Wid Akeel Awadh[*] [2]Ali Salah Hashim [1]Alaa Khalaf Hamoud

[1]Computer Information System Department- College of Computer Science and Information Technology- University of Basrah, Iraq
[2]Computer Science Department- College of Computer Science and Information Technology- University of Basrah, Iraq

[*]**Email:** umzainali@gmail.com

Abstract:-

One of the latest trends in IT sector is cloud computing. It develops the capabilities of organizations dynamically without training new employees, obtaining new software licenses or investing in infrastructure. At present, user keeps and share a high amount of data on cloud, and hence, the security of cloud computing is necessary so that there is no threat to any of the user's data. Steganography is becoming a standard practice for both cloud users and cloud service providers as a mechanism against unauthorized surveillance. Steganography refers to writing hidden messages in a way that only the sender and receiver have the ability to safely know and transfer the hidden information in the means of communications. The aim of this paper is to provide an overview of steganography in cloud computing and compare various studies on the basis of technique selection, carrier formats, payload capacity and embedding algorithm to open important research directions.

Keywords: Cloud Computing, Steganography,Data security, Cryptography.

Introduction:-

Over the last few years, a cloud computing has become a tendency in information technology (IT) as it promises significant to reductions the costs and new business chance for its users and providers (Kaur *et al.*, 2015). Cloud computing is defined by the National Institute of Standards and Technology (NIST) as : "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"(Peter Mell, 2011).

Even though cloud computing applications are only at the development phase, significant barriers that are related with adopting cloud computing, such as security issues, compliance and legal matters (Hussain *et al.*, 2017). Two techniques are developed to protect the information: steganography and cryptography. Steganography is often confused with cryptography although the two are completely different terms. Cryptography manages privacy, while steganography manages secrecy (Ahmed *et al.*, 2017).

Steganography is the science of securing information among a carrier object such that solely the sender and receiver have the power to recognize and observe the hidden information and safely transfer it through the means of communications. Steganography is a combination of two words Stegano+Graptos. Stegano means "covered" and graptos means "writing" which exactly means "covered writing"(Yogeswari *et al.*, 2016). While, the study of means of converting information from its normal form into a coded format is called cryptography (Muthulakshmi *et al.*, 2016).

The objective of this paper is to describe carefully the steganographic techniques demonstrated in cloud computing and compare these studies on the basis of technique selection, capacity, carrier formats and embedding algorithm. Technique selection is used to ensure security through steganography, cryptography and compression. However, the second criterion point to the maximum size of secret message that can be hidden without retracting the quality of the cover. In addition, carrier formats refer to which cover is used to

embed the secret message. Furthermore, an embedding algorithm is used to ensure image quality (imperceptibility), which is responsible for maintaining an image quality that is the same as the original. This objective can be achieved by keeping the pixel value as similar to the original as possible.

Cloud Computing:-

Cloud computing is considered as a new paradigm in the field of IT. It is a consequence of developments in distributed computing, systems management, hardware technologies, and Internet technologies(Bokhari *et al.*, 2016). It provides a number of services including applications, storage servers, and networks. Because of convenience and on-demand services, today many organisations are employing it(Garg *et al.*, 2019). Cloud computing is classified into three services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) as showed in Figure 1.

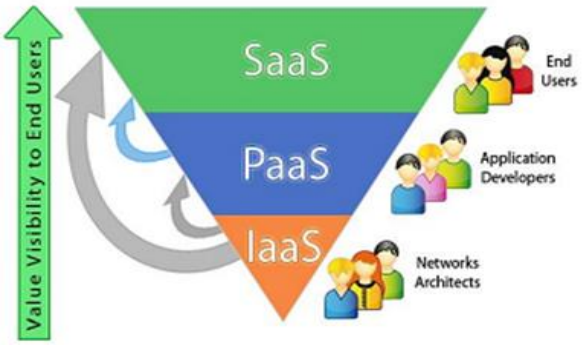

Figure 1: Structure of cloud computing services(Awadh *et al.*, 2018)

- SaaShas changed the concept of software as a product to that of a service instead. The software runs in the cloud and the users can access it via the Internet to work on an application. Previous studies pointed out that SaaS includes some processes that enable the service providers to provide application that can be rented on the Internet. Many companies are using and providing these services this include for example Google Apps (Hashim *et al.*, 2014).
- PaaSenables powerful tools for developers to create the applications, without having concerns about the infrastructure. The PaaS category represents clouds that access a range of computer, database, and storage functions within a virtualized platform provided over the internet and services released by providers such as Salesforce.com, Microsoft Azure, and Google App Engine(Stergiou *et al.*, 2018).
- IaaSis the highest service layer in the cloud computing service structure.This model represents the infrastructure responsible for storage, operating systems, applications, information and data as well as the network requirement to connect between cloud services. Therefore, IaaS consists of systems hardware and storage resources (Abdelaziz *et al.*, 2018).

Many researchers classify the deployment approaches of cloud computing into four primary categories which are; Private, Public, Hybrid, and community. Compared with the public cloud, the private cloud can ensure physical security and is safer because of its specific internal exposure, where its resources and applications can be accessed only by the organisation itself (Modi *et al.*, 2017).While hybrid cloud is an integration of two or more abovementioned cloud infrastructures. The importance of this model is that it often offers extra resources with high security (Kaisler *et al.*, 2012). And the community cloud is used by organisations sharing their cloud infrastructure among customers who have similar interests such as policy, security requirements, mission and compliance considerations. (Ali *et al.*, 2015).

Security Challenges in Cloud Computing:-

Cloud naturally raises new security challenges for the following reasons(Garg *et al.*, 2016):

1. Traditional encryption basics for data security protection cannot be strictly followed because users lose control of data under cloud computing. With the different data per user stored in the cloud and the demand for continuous data security, data storage validation in the cloud becomes a challenging task.
2. Data stored in the cloud may be frequently updated by the users through deletion, insertion, appending,modifying and reordering. Thus, ensuring theauthenticity of storage for updating dynamic data is important.
3. The evolution of cloud computing is conducted through data centres operating simultaneously in a distributed manner throughcollaboration.

Overview of Steganography:-

The first description of steganography dates back to ancient Greece. Steganography has also been

used during the Cold War period for secure communication. At present, various algorithms are used to protect confidential information conveyed through with different media carriers(Cheddad *et al.*, 2010). In general, steganography is the process of sending secret messages to multiple parties that avoid the enemy from knowing its actual content. The result providesa file called stego object, which contains the secret message. This stego file is sent to the receiver who then restores the message by applying the extracting algorithm (AL-Mozani *et al.*, 2012). The general steganography process is illustrated in Figure2.

-

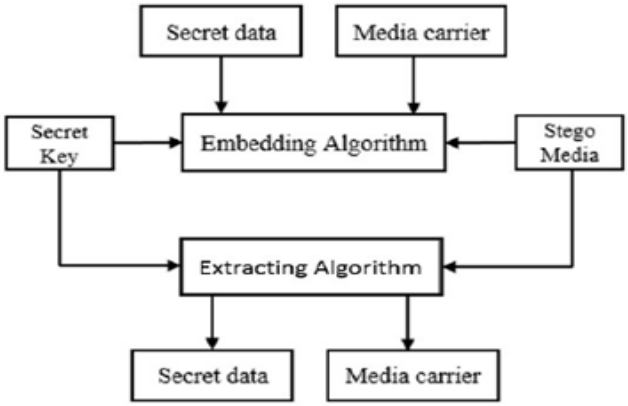

Figure 2: Block diagram of steganography process (Choudry *et. al.*, 2015)

The basic steganography model consist from four component:

1. Media carrier: Also called cover object, this is used to carries the secret message and prevent anyone from noticing the presence of actual useful information.
2. Secret data: A secret message can be of any type such as text, image, video, and audio.
3. Secret key: A secret key is used to encrypt / decrypt the hidden message.
4. Stego media: Also called stego object, this is the result obtained after embedding the secret message.

Types of Steganography:-

Five main categories of file formats can be used for steganography, as shown in Figure3.

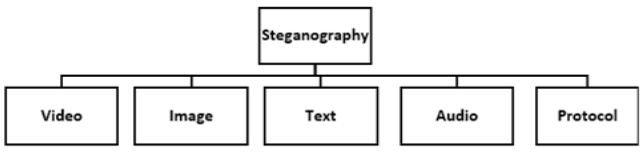

Figure 3: Types of Steganography(Saber, 2013)

1. Video steganography: In this type of steganography used Video format to hide secret information. Where Video files consist of a collection of images and audio. The use of video steganography is preferable to the other multimedia files because it is more effective and efficient in hiding information within information. In general, most of the proposed techniques on audio and images can be implemented to video files as well. Many types of video files can be used such as H.264, Mp4, MPEG, AVI or other video formats(Awadh, 2016).
2. Image steganography: Digital images are popular over the Internet because they aremostly used as the cover object for steganography. In this type, a secret message is hidden in a digital image using an algorithm througha secret key to create a stego image. Generally, pixel intensities are used to hide secret information (Banerjee *et al.*, 2014).
3. Text steganography: Embedding secret information in a text file is known as text steganography. This method is used to store text file only therefore the required memory is less. In text steganography, a number of white spaces, tabs and capital letters are used to perform message hiding. This type of steganography is not commonly used because text files containing a large amount of redundant data (Lwin *et al.*, 2014).
4. Protocol steganography: In this technique, thesecret information is embedded within networkprotocols such as TCP, UDP, ICMP and IP, whereprotocol is used as a carrier. A network packetconsists of packet headers, user data and packettrailers. Thus, steganography can be used in some layers of the network model. This term isknown as protocol steganography (Dimitrova *et. al.*, 2017).

Literature Review:-

In this section we will discuss the most important techniques of steganographic that have been used in the data security of cloud computing published in period from 2016 to 2018.In (Awadh *et. al.*, 2017), the author proposed available steganographic technique for enhancing data security in cloud. The proposed technique applies the matrix of location (MoF)to enhance security.In addition, this text file covers the message they want to conceal using the steganographic method, thereby resulting ina natural text file.Thus, people cannot see the text that shrouds the message inside. This model satisfies high capacity, security and

robustness requirements.In this study(Rani *et. al.*, 2017), the authors increased cloud storage security using steganography, encryption decryption techniques, compression and splitting technique to overcome the limitations of traditional data protection algorithms. To keep the data secure from attackers, the data are hidden inside the image using the least significant bit(LSB) technique. For security enhancement, a split algorithm is implemented, which can divide thelong file into different parts and store the parts on different clouds.Furthermore,this method can perform encryption and decryption. The results of this study show that the proposed technique provides high data security andhigh-quality services to the users better than the existing technique with regard to encryption and decryption times.In this study(Saini *et. al.*, 2014),data security in cloud computing are enhanced by merging three algorithms.Digital signature algorithm (DSA), verification of data and authentication are applied.After that, for data encryption, a data encryption standard (DES) algorithm is used.Finally,the steganography technique is used to provide high-level security for the data.This approach fulfils security and authenticity requirements. However, the complexity of time is high. In (Abdulkarim, 2017), the authors proposed a technique to improve the cloud security system using Rivest–Shamir–Adleman (RSA) algorithm as digital signature and image steganography. The RSA algorithm is used to provide a message digest to authenticate the user by generating public and private keys, which are used for authentication and not repudiation. Once the data have been authenticated, they are concealed using image steganography to ensure smooth transfer without drawing the attention of intruders. The researchers considered memory storage, network bandwidth, CPU processing time and power as metrics.In (Ranjan *et. al.*, 2016), the authors proposea new technique for sharing and saving confidential information into the cloud by utilising multilayer steganography (through Hash–LSB technique) and AES cryptography algorithm,thereby enabling clients to enhance the privacy of secret data, such as personnel, bank and health information and others,when they are stored inthe cloud.Concurrently, all stored data are available in any time and from anywhere.In (Manjunath *et. al.*, 2017), the researchers present a novel reversible data-hiding scheme in video for the cloud environment. In this method, the secret image is hidden inside a cover video by the modified histogram method, thereby providing security to the data. An examination ofthe proposed technique shows that ithas fulfilled the objectives of authentication, security and robustnessneeded in any steganography technique for hiding images. In (Suneetha *et. al.*, 2017), after investigating the security problem in cloud computing, the authors propose an efficient stenographic strategy to support thedata security atrest. In this technique, the first and last bits of image are extracted from odd pixel values of an image file. This image covers the message to be hidden using the steganographic method, to produce an image similar to the original. So, people cannot see the hidden message inside it. The main objective of the proposed algorithm is to guarantee the data integrity at the data centre of cloud provider. It is worth mentioning, this strategy using in small environment and with a limited number of security threats.In (Mohis*et. al.*, 2016), the authors proposed a mediated certificate less public key encryption (mCL–PKE) scheme, which provides precise security to data stored in the public cloud, is introduced. This technique addresses the key escrow issue and the certificate revocation problem. In this method, the sensitive data shared by the organisations were embeddedin an image and uploaded to the cloud through LSB encoding,thereby providing additional security to the data. When an attacker learns the secret data inside the cloud, only the image can be visible. The overhead is reduced on the owner's side by implementing encryption only once for all information.In (Mary *et. al.*, 2017), the problem of authorised access in cloud storage can be solved by merging the obfuscation technique with steganography. The main principle of obfuscation is to convert data into a new form and conceals the original data while the existence of information is hidden by using the steganography. A magical rolling alpha-digit obfuscation (MRADO) techniqueis used to mask the data.Then,the masked data are hidden in the image using the least significant bit (LSB) substitution method. The hybrid technique offers high capacity and quality.In (Mahajan, 2017), a novel technique is suggested, so this technique canbe provide security to cloud computing by authenticating the user. This algorithm is able to dispatch the encrypted data to the supplier, who can similarly apply the security by encrypting the client's data. Thus, the client's data are secure at both ends. The proposed algorithm, used a security algorithms (LSB and RSA), with steganography technique to store encrypted data in the image.The main objective from used the proposed algorithm, is to provide an encrypted manner to control

the sending of data from the client to the supplier. The supplier alsoprotects the data from unauthorised access by using a security algorithm.In (Palathingal *et. al.*, 2018), this project deals with security problems in cloud computing systems and how they can be prevented.Therefore, both cryptography and steganography methodsare usedto enhance data security. Based on the idea that the RSA algorithm is the most secure of algorithms, the integration of other algorithms with RSA is conducted. In the steganography process, an encrypted image is derived, which appears to be identical to the original image when viewed by the human eye. The differences can be observed if analyse the image binary codes.

Evaluation of Steganography:-

There are four objectives and an evaluation of strong and weak points that must be considered when creating a steganographic method (Hashim *et. al.*, 2018):

1. Capacity: is the maximum numbers of secret messages bits that can be embedded in the cover without loss the quality of cover.
2. Security: is one of the most important evaluation standards in steganography. A good steganographic technique should be proof tosteganalysis attacks.
3. Imperceptibility: refers to the transparency and quality of an image. After hiding a secret message into the cover image, transparency and quality are degraded into a stegoimage compared with a coverimage. Thus, the stego image should appear similar tothe original image. The performance of thestego image can be measured by peak signal-to-noise ratio (PSNR), which can be calculated by the difference of distortion between the cover and stego images. PSNR is defined asthe equation(1):

$$PSNR = 10 \log 10 \left(\frac{C2_{max}}{MSE}\right), \quad (1)$$

Where MSE indicatesthe mean square error (MSE) defined asthe equation(2):

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2, \quad (2)$$

Where x and y are the coordinates of the coverimage, M and N are the dimensions of the cover image, (S_{xy}) is the generated stegoimage and (C_{xy}) is the cover image.

4. Computational:complexity measures the cost and complexity of embedding and extracting a hidden secret message.

This review has described steganography in cloud computing. Thus, the frequency domain is not included in this review.

Challenges and Open Research Issues:-

Many studies on steganography in cloud computinghave been published.However, few of them focus on improved file quality, while others are aimed at payload capacity or providingenhanced security. The aim of those works is to obtain a robust method, while the others can be used only to check the effect of the method on different attacks.According to the related research, the challenges and open issues in this field necessitate accepting the use of steganography incloud computing and detecting the weak points and drawbacks by developing new robust techniques (Mahmood *et al.*, 2017).A summary of the main features of the steganography techniques in cloud computingis shown in Table 1.

Table 1: Summary of main features

	Technique											Carrier Formats				Issue		
	Steganography				Cryptography						Compression							
Reference	MoF	LSB	Histogram method	MSB	AES	DSA	DES	RSA	mCL-PKE	MRADO	2D-DWT	GZIP	Video	Audio	Image	Text	Capacity	Security	Quality
(Awadh *et. al.*, 2017)	✓															✓	✓	✓	✓
(Rani *et. al.*, 2017)		✓			✓							✓			✓			✓	✓
(Saini *et. al.*, 2014)		✓				✓	✓							✓				✓	✓
(Abdulkarim, 2017)		✓						✓							✓		✓	✓	
(Ranjan *et. al.*, 2016)		✓			✓			✓							✓			✓	✓
(Manjunath*et. al.*, 2017)			✓										✓				✓	✓	✓
(Suneetha*et. al.*, 2017)		✓		✓											✓				✓
(Mohis *et. al.*, 2016)		✓							✓						✓			✓	✓
(Mary *et. al.*, 2017)		✓								✓					✓		✓	✓	
(Mahajan, 2017)		✓						✓							✓		✓	✓	✓
(Palathingal et al., 2018)								✓			✓				✓			✓	

Conclusion:-

This paper has presented a preliminary systematic literature review of various cloud computing techniques. Cloud computing is an emerging

technology that presents numerous benefits but raises security challenges. The latest related development is steganography, which is the technique of hiding information in a scenario where the cloud is used by many users whose data are frequently synchronised to the cloud. Steganography can be used on networks to ensure data security without third-party interference. Thus, we can conclude that differencesexist in the complexity of implementation among the reviewed techniques, and each technique has its own weak and strong points.

References:-

Abdelaziz, A., Elhoseny, M., Salama, A. S., & Riad, A. (2018). A machine learning model for improving healthcare services on cloud computing environment. *Measurement*, *119*, 117-128.

Abdulkarim, A. I., and Boukari Souley. (2017). An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography. *International Journal of Scientific & Engineering Research*, *8*(7).

Ahmed, O. M., & Abduallah, W. M. (2017). A Review on Recent Steganography Techniques in Cloud Computing. *Academic Journal of Nawroz University*, *6*(3), 106-111.

AL-Mozani, A. S. S., & Awadh, W. A. J. (2012). A New Text Steganography Method by Using Non-Printing Unicode Characters and Unicode System Characteristics in English/Arabic documents. *JOURNAL OF THI-QAR SCIENCE*, *3*(3), 192-200.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, *305*, 357-383.

Awadh, W. A. (2016). A Novel Approach for Hiding Information in Text Steganography. *International Journal of Scientific & Engineering Research*, *7*(12).

Awadh, W. A., and Ali S. Hashim. (2018). Investigation of Security and Privacy Methods for Public Mobile Cloud Computing. *Journal of Engineering and Applied Sciences*, *13*(12), 4396-4402.

Awadh, W. A., & Hashim, A. S. (2017). Using Steganography for Secure Data Storage in Cloud Computing. *International Research Journal of Engineering and Technology*, *4*(4), 3668-3672.

Banerjee, I., Bhattacharyya, S., & Sanyal, G. (2014). *Robust image steganography with pixel factor mapping (PFM) technique.* Paper presented at the Computing for Sustainable Global Development (INDIACom), 2014 International Conference on.

Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K. (2016). *Cloud computing service models: A comparative study.* Paper presented at the Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on.

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal processing*, *90*(3), 727-752.

Choudry, K. N., & Wanjari, A. (2015). A Survey Paper on Video Steganography. *International Journal of Computer Science and Information Technologies*, *6*(3), 2335-2338.

Dimitrova, B., & Mileva, A. (2017). Steganography of Hypertext Transfer Protocol Version 2 (HTTP/2). *Journal of Computer and Communications*, *5*, 98-111.

Garg, N., & Kaur, K. (2016). Hybrid information security model for cloud storage systems using hybrid data security scheme. *International Research Journal of Engineering and Technology (IRJET)*, *3*(4), 2194-2196.

Garg, P., Sharma, M., Agrawal, S., & Kumar, Y. (2019). *Security on Cloud Computing Using Split Algorithm Along with Cryptography and Steganography*. Paper presented at the International Conference on Innovative Computing and Communications.

Hashim, A. S., & Othman, M. (2014). Cloud Computing Adoption by Universities: Concepts and Review. *International Journal of Science and Research (IJSR), 3 (2): 348, 353*.

HASHIM, M., RAHIM, M., SHAFRY, M., & ALWAN, A. A. (2018). A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN. *Journal of Theoretical & Applied Information Technology*, *96*(4).

Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing.

Applied Computing and Informatics, 13(1), 57-65.

Kaisler, S., Money, W. H., & Cohen, S. J. (2012). *A decision framework for cloud computing.* Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

Kaur, R., & Kaur, J. (2015). *Cloud computing security issues and its solution: A review.* Paper presented at the Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on.

Lwin, T., & SUWAI, P. (2014). Information Hiding System Using Text and Image Steganography. *International Journal of Scientific Engineering and Technology Research, 3*(4), 1972-1977.

Mahajan, N., Arora M., and Chopra Sh. (2017). Framework for cloud data security *International Journal of Computer Science and Engineering*.

MAHMOOD, A. S., RAHIM, M., & SHAFRY, M. (2017). GENERATING AND EXPANDING OF AN ENCRYPTION KEY BASED ON KNIGHT TOUR PROBLEM. *Journal of Theoretical & Applied Information Technology, 95*(7).

Manjunath K. K. and Sanjeev R. K. (2017). Manjunath K. K. and Sanjeev R. K, . *International Journal of Emerging Research in Management &Technology*.

Mary, B. F., & Amalarethinam, D. G. (2017). *Data Security Enhancement in Public Cloud Storage Using Data Obfuscation and Steganography.* Paper presented at the 2017 World Congress on Computing and Communication Technologies (WCCCT).

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. *The journal of supercomputing, 63*(2), 561-592.

Mohis, M., & Devipriya, V. (2016). *An improved approach for enhancing public cloud data security through steganographic technique.* Paper presented at the Inventive Computation Technologies (ICICT), International Conference on.

Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., & Ullah, A. (2017). Cloud Computing Environment and Security Challenges: A Review. *International Journal of Advanced Computer Science and Application, 8*(10), 183-195.

Muthulakshmi, P., Shathvi, K., Aarthi, M., & Seethalakshmi, V. (2016). Encrypted Image With Hidden Data Using AES Algorithm. *International Journal of Science, Engineering and Technology, 5*(4).

Palathingal, A. G., George, A., Thomas, B. A., & Paul, A. R. (2018). Enhanced Cloud Data Security using Combined Encryption and Steganography.

Peter Mell, a. T. G. (2011). The NIST Definition of Cloud Computing, Recommendations of The National Institute of Standards and Technology.

Rani, K., & Sagar, R. K. (2017). *Enhanced data storage security in cloud environment using encryption, compression and splitting technique.* Paper presented at the Telecommunication and Networks (TEL-NET), 2017 2nd International Conference on.

Ranjan, A., & Bhonsle, M. (2016). Advanced System to Protect and Shared Cloud Storage Data using Multilayer Steganography and Cryptography. *International Journal of Engineering Research, 5*(6), 434-438.

Saber, A. S. (2013). Steganography in MS Excel Document Using Unicode System Characteristics. *Journal of Basrah Researches (Sciences), 39*(1A), 10-19.

Saini, G., & Sharma, N. (2014). Triple security of data in cloud computing. *International Journal of Computer Science and Information Technologies, 5*(4), 5825-5827.

Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*, 964-975.

Suneetha, D., & Kumar, R. K. (2017). A Novel Algorithm for Enhancing the Data Storage Security in Cloud through Steganography. *Advances in Computational Sciences and Technology, 10*(9), 2737-2744.

Yogeswari, G., & Eswaran, P. (2016). *Enhancing Data Security for Cloud Environment based on AES Algorithm and Steganography Technique.* Paper presented at the Proceeding of the International Conference on Innovations in Computer Science & Technology (ICICST-2016), page (s).