A Review on Recent Steganography Techniques in Cloud Computing

Omar M. Ahmed[1], Wafaa M. Abduallah[2]

[1]Department of Computer Science, Faculty of Science, Zakho University, Duhok, Kurdistan Region – Iraq
[2]Department of Computer Science and Information Technology, College of Computer Science & Information Technology, Nawroz University, Duhok, Iraq

ABSTRACT

As with the growth of information on the cloud, cloud security is seen as more essential than before. Presently, millions of users are utilizing the cloud. The security of cloud computing is urgently required, where data are being transmitted or transferred between the users and servers. Steganography is considered as the most effective techniques for securing the communication in the cloud. 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. This paper review some of the recent steganography techniques that have been proposed to improve the security of data in the cloud and to make it more immune to cyber-attacks and eavesdropping.

KEYWORDS: Steganography, Cloud Computing, Security, Privacy.

1. INTRODUCTION

As a result of excessive developments in digital technology and network, it has turned out to be extremely well-known and popular to transmit the data from one end to another over web and cloud computing. Cloud computing is a model for allowing advantageous, on-request organize access to a common pool of configurable computing assets (e.g., applications, storage, servers, and networks) that can be immediately provisioned and discharged with minimal management efforts or specialist organization communications (C. Yang, Lin, & Liu, 2013). Hence, a problem of data vulnerability to threat and attack is raised. So, the communication of data should be secure and along with these lines, the significance of information security has been primarily expanded. Information security can be accomplished by utilizing cryptography and steganography methods. Steganography is regularly confused for Cryptography, in spite of the fact that they are truly different terms. Cryptography manages the privacy while steganography manages the secrecy.

Academic Journal of Nawroz University (AJNU)
Volume 6, No 3(2017), 6 pages
Received 1 May 2017; Accepted 1 August 2017
Regular research paper: Published 29 August 2017
Corresponding author's e-mail: Omar.m@gmail.com

"signature-based System (SBS) and Anomaly-Based System (ABS)". The first type (SBS) depends on different techniques of pattern recognition for preserving the database; it uses the signatures of formerly identified attacks and then comparing them with the previously investigated data. When the matching is occurred, an alerting flag is raised to announce the matching. In contrast, the ABS systems secures the substance of message by changing them into cipher content through some cipher techniques with or without utilizing a key. So far it gives the output that is unreadable and scrambled, as it may, sufficiently suspicious to pull in interceptors' consideration. While, steganography hides the existence of secret data during transmission (Abduallah & Rahma, 2016).

The objective of this paper is to review the techniques of steganography that are used with cloud computing to make it more secure and immune to cyber-attacks and eavesdropping.

1. Cloud Computing and It's Security

In the field of Information Technology, Cloud computing is considered as a new paradigm. It is a consequence of developments in distributed computing, systems management, hardware technologies, and Internet technologies (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009). It is a dynamic technology platform that tends to an extensive variety of requirements by giving cyber-infrastructure to keep up and broaden data storage abilities. As well as, cloud

computing gives access to hardware and software without significant capital speculation and gives simpler access to services and applications that can be acknowledged with insignificant service provider interaction. This has empowered cloud computing to be created as a technological development that can deal with a lot of data that are exchanged and stored by means of electronic applications (C. L. Yang, Hwang, & Yuan, 2012).

Cloud computing is separated into three layers by researchers: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) as showed in Figure 1. (Bokhari, Shallal, & Tamandani, 2016).

Fig 1. Structure of cloud computing

Software as a Service (SaaS), this layer enables the clients to rent and utilize the applications from the supplier without mount it on their own computer. This is mean the authorized applications which been given to clients are running on cloud's basis through the interface of a thin or thick client, for example, internet explorer, Google chrome, and numerous others. SaaS is a service where the real development of applications and software happens on the stages given by the PAAS layer. SaaS layer is primarily worried about end users for the reason that end users can get to and utilize these applications which were made by cloud suppliers.

Platform as a Service (PaaS), this layer gives an appropriate situation or platform in which the developer can build up the software and applications to send them through the web with no requirement for mount or deal with the environment of development. PaaS is enabling the client to rent virtualized servers and connected services for execute accessible applications or create and test the better and brighter one. The client does not control over the cloud's basis, for example, OS, stockpiling, systems, or servers, while the client has the control over the sent applications and their setups.

Infrastructure as a Service (IaaS), this layer gives the raw hardware and virtual infrastructure in order to have the ability to create, manage and destroy storage, and VMs through network-based service. IaaS layer is an outcome for the development of virtual private server which been as of now known since several years back. The supplier of IaaS is providing the client with virtual server alongside at least one CPU executing a few decisions of operating. The VM could be rented as long as it required. The infrastructure resources can scale all over as indicated by client's request and will be charged rely upon the amount, duration, and additional services which been utilized by the client from the VM. So as to serve the client the supplier is responsible for maintaining, hosting, and operate the infrastructure. The client has the ability to control over the OS, deployed applications, storage, Memory, CPU, IP address, and some limit quantity of certain components of the networking.

Many researchers characterize the deployment approaches of cloud computing into four primary classifications which are; Private, Public, Hybrid, and community. Private cloud is expensive but more secure than Public cloud and less accessible. While the hybrid blended between the high security and the affordability. And the community cloud is an incorporation between some organizations to utilize the cloud technology. Every deployment model has its advantages and disadvantages. The choice of picking an appropriate cloud computing deployment model ought to consider organizational and additionally technological factor (Patidar, Rane, & Jain, 2011).

For many reasons, new challenging security threats the Cloud Computing is naturally raised. Firstly, traditional cryptographic fundamentals for the protection of information security can't specifically abide because of the not controlling the information by clients under Cloud Computing. Thus, confirming the capacity of accurate information in the cloud must be performed without clear knowledge of the entire information. Considering distinctive information for each client saved in the cloud and the request of nonstop information security, the issue of checking rightness of information

storing in cloud turns out to be all the more challenging. Secondly, this kind of Computing is not an information distribution center by the third party. By the users in the cloud, the stored data may be regularly updated, which contain reordering, modifying, appending, insertion, deletion, etc. To guarantee the accuracy of storage for updating of dynamic information is of much significance. Last however not the least, the development of Cloud Computing is finished by data centers running at the same time, with cooperation and in distributed manner (Garg & Kaur, 2016).

2. Related Works

Many research works have been conducted in the literature for securing data in the cloud. In this section, most of the recent steganographic techniques that are implemented to secure the data in the cloud are presented. More specifically, In (Sarkar & Chatterjee, 2014) the authors proposed a viable and effective steganographic technique for upgrading security on data-at-rest. At the point when the data are stored in the cloud data center, nobody can see the first substance of the data with no appropriate identification. Through detailed security and execution investigation, the proposed model nearly guarantees the integrity of data when it is established in the data center of any Cloud Service Provider (CSP). But this technique can deal with just a limited quantity of security threats in a small environment.

In (Saini & Sharma, 2014) the researchers by merging three algorithms enhanced the security of data in cloud computing, initially for authentication and verification of data, Digital signature algorithm (DSA) is applied. Then for data encryption, an Advanced Encryption Standard (AES) algorithm is applied and finally, the last step of this system was to hide data within an audio file using Steganography technique for providing most extreme security to the data. This system fulfills both security and authenticity but because it is a one by one process the time complexity is high.

In (Saravanakumar & Arun, 2014) for providing security to cloud computing, the authors developed an algorithm to develop a client owned security model. This algorithm has the ability for dispatching the encrypted data to the supplier. The supplier can similarly by using the algorithm applies the security by encryption of the client's data. At both the end the client's data is secure. The proposed algorithm together with steganography also uses ASCII and BCD security that stores the encoded data in an image file. Also, they use Common Deployment Model (CDM) algorithm over the cloud which gives interoperable security services. For the proposed algorithm, the major objective is in an encrypted manner to send and control the data by the client to the supplier. The supplier as well keeps up the data with a security algorithm from unauthorized access the data to be protected.

In (Pant, Prakash, & Asthana, 2015) the authors proposed to use steganography and cryptography technique with each other for securing data. They think that RSA algorithm is the most secured one among other algorithms. For providing more security to data they integrate other algorithms with RSA algorithm. An encrypted image gets it in steganography process, which appears to be identical to the original image by human eye. The differences would be seen If we analysis the image binary codes. Otherwise, the original image can't be recognized. The approach they have used in their paper, for the security of data in cloud computing field or the web it will make a solid structure.

In (Nimmy & Sethumadhavan, 2014) for cloud computing the authors proposed an important verification authentication scheme with many security features such as password change option, session key agreement between the users and the cloud server, and mutual authentication. This proposed scheme with using steganography and secret sharing they presents an innovative way of authentication. Out-of-band authentication gives people communication which makes the protocol better in a way that no supplementary software or hardware or training is needed for the end user. Furthermore, resource constrains of cloud computing are given less urgency to provide high security to the cloud. Many popular attacks can be resisted by the proposed protocol such as man in the middle attack, denial of service attack, and replay attack.

In (Sarvabhatla, M.Giri, & Vorugunti, 2014) the authors have cryptanalysis the "Novel mutual authentication protocol for cloud computing using secret sharing and steganography" proposed by (Nimmy & Sethumadhavan, 2014). They have demonstrated that this scheme is powerless against different attacks and there is an extension for diminishing the substantial weight of cryptographic operations on resource weaken the client side. They have proposed the enhanced scheme after which, they removed the resource exhausting encryption, decryption, and stegano operations from the client side. With their scheme, the weight on the servers is diminished definitely which brings the faster reaction to clients from the server side. When analyzing security quality of their scheme it shows that it is resistant to all main cryptographic attacks. These two advanced the resistant to all major cryptographic attacks and Less computation requirement from client side makes their scheme further adaptable and practical to usage regardless of resource constrained devices like tabs, mobile etc.

In (Mandai & Bhattacharyya, 2015) they propose a system to address installed classified data in an image similarly of image steganography, however, here an extra technique is utilized to pick pixels of cover image where

the classified data will be hidden. Before hiding the data on the cover image, a technique for privacy encrypts the classified data using Cryptography and GA. They propose a data position scrambling PMM and genetic algorithm based secret key image encryption method. After the proposed technique is investigated, plainly this encryption technique is fulfilled the objectives that are needed in any encryption technique for encrypt content or image.

In (Mohis & Devipriya, 2016) they propose a public key encryption scheme which is a mediated certificate-less encipherment scheme. For the public cloud, it gives unambiguous security. This technique in the public cloud takes care of the key escrow issue and also certificate revocation problem. Notwithstanding this encryption scheme here incorporated an inserting module for upgrading the security. In this method, the sensitive data is hiding inside an image shared by the organizations, in this way for the attackers the secret data will be hidden. Just the image will be obvious to the unapproved clients subsequently the security can be improved. When different clients are utilizing same arrangements of access control then this technique can perform encipherment only once for each information. Henceforth the general overhead at the proprietor side can be decreased. Implanting module with Steganography decreases unauthorized access of attackers on the sensitive data.

In (Murakami, Hanyu, Zhao, & Kaneda, 2013) the authors proposed a technique for development of security in cloud framework with using of steganography. In the proposed technique, they applied the dynamically generated morphing image for enhancement of security, and this image covers the message which they want to conceal. This is use of steganographic method, and the output is a natural image, so people can't see the image shrouds the message inside. Furthermore, this morphing image is produced dynamically, and for decrypting there is no keys. Other than this method, they characterized a few principles of working condition for development of security.

In (Ke & Dong-qing, 2012) the authors proposed for 3D point cloud models, a new adaptive steganography with high capacity, low robustness and distortion against relative changes and vertex reordering attack. The proposed scheme accomplishes a productive change of implanting imperceptions by utilizing normal direction of vertexes to assess the embedding capacity of each vertex to accomplish adaptability and low distortion, by means of consideration to the human visual system.

In (Ranjan & Bhonsle, 2016) the authors presented new steps for sharing and storing the data in adequately way utilizing multilayer steganography by utilizing AES cryptography alongside information proprietor control to internal or external clients. Presently, clients have much more privacy for storing secret data such as personnel health info, certificate, bank info and so on into the cloud. At the same time, this all stored data will be reachable at any time any location over the globe.

The summary of all previous literature overview is presented in Table 1.

Table. 1. Using Steganography in Cloud Computing

Authors	Year	Title	Used Algorithms
Sarkar & Chatterjee	2014	"Enhancing Data Storage Security in Cloud Computing Through Steganography"	
Saini & Sharma	2014	"Triple Security of Data in Cloud Computing"	DSA DES
Saravanakumar & Arun	2014	"An Efficient Ascii-Bcd Based Steganography for Cloud Security Using Common Deployment Model"	ASCII Based SteganoEncryption ASCII Based SteganoDecryption
Pant, Prakash, & Asthana	2015	"Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques"	StegoTools (rRMS) RSA
Nimmy & Sethumadhavan	2014	"Novel mutual authentication protocol for cloud computing using secret sharing and steganography"	secret sharing
Sarvabhatla, M.Giri, & Vorugunti	2014	"A Secure Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography"	secret sharing

Mandai & Bhattacharyya	2015	"Secret Data Sharing in Cloud Environment Using Steganography and Encryption Using GA"	PMM (Pixel Mapping Method) GA (Genetic Algorithm)
Mohis & Devipriya	2016	"An improved approach for enhancing public cloud data security through steganographic technique"	mediated certificateless public key encryption (mCL-PKE)
Murakami, Hanyu, Zhao, & Kaneda	2013	"Improvement of security in cloud systems based on steganography"	dynamically generated morphing image
Ke & Dong-qing	2012	"An Adaptive Steganography for 3D Point Cloud Models"	adaptive steganography
Ranjan & Bhonsle	2016	Advanced technics to shared & protect cloud data using multilayer steganography and cryptography	multilayer steganography AES Hash-LSB

3. Conclusion

At this point, several techniques proposed by some authors are explored in various literature. Steganography is the newest improvement in addition to a very overstated technique of hiding the data where the cloud is frequently utilized by all clients and their information will keep synchronized to the cloud almost whenever. This steganography technique without using third party interference for data security can be used on networks.

So, it can be concluded that there is a difference in complexity of implementation between the reviewed techniques and each of them have its own strong and weak points. Contingent on the necessity of a particular application, for different applications using different steganography techniques.

REFERENCES

Abduallah, W. M., & Rahma, A. M. S. (2016). A Review on Steganography Techniques. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, 131–150.

Ahamad, T., & Aljumah, A. (2014). Cloud Computing and Steganography – Attack Threat Relation. *MAGNT Research Report*, *2*(4), 1444–8939.

Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K. (2016). Cloud computing service models: A comparative study. *IEEE 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 16–18.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, (July), 1. https://doi.org/10.1109/CCGRID.2009.97

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.

Ke, Q., & Dong-qing, X. (2012). An Adaptive Steganography for 3D Point Cloud Models. *IEEE 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*.

Mandai, S., & Bhattacharyya, S. (2015). Secret Data Sharing in Cloud Environment Using Steganography and Encryption Using GA. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 1469–1474. https://doi.org/10.1109/ICGCIoT.2015.7380699

Mazurczyk, W., & Szczypiorski, K. (2011). Is cloud computing steganography-proof? *Proceedings - 3rd International Conference on Multimedia Information Networking and Security, MINES 2011*, 441–442. https://doi.org/10.1109/MINES.2011.95

Mohis, M., & Devipriya, V. S. (2016). An improved approach for Enhancing Public Cloud Data Security through Steganographic Technique. *IEEE In Inventive Computation Technologies (ICICT)*.

Murakami, K., Hanyu, R., Zhao, Q., & Kaneda, Y. (2013). Improvement of security in cloud systems based on steganography. *2013 International Joint Conference on Awareness Science and Technology & Ubi-Media Computing (iCAST 2013 & UMEDIA 2013)*, 503–508. https://doi.org/10.1109/ICAwST.2013.6765492

Nimmy, K., & Sethumadhavan, M. (2014). Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography. *2014 Fifth International Conference on the Applications of Digital Information and Web Technologies (Icadiwt)*, 101–106.

Pant, V. K., Prakash, J., & Asthana, A. (2015). Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques. *2015*

International Conference on Green Computing and Internet of Things (ICGCIoT), 490–494. https://doi.org/10.1109/ICGCIoT.2015.7380514

Patidar, S., Rane, D., & Jain, P. (2011). A survey paper on cloud computing. *Proceedings - 2012 2nd International Conference on Advanced Computing and Communication Technologies, ACCT 2012*, 394–398. https://doi.org/10.1109/ACCT.2012.15

Ranjan, A., & Bhonsle, M. (2016). Advanced technics to shared & protect cloud data using multilayer steganography and cryptography. *IEEE 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, 35–41.

Saini, G., & Sharma, N. (2014). Triple Security of Data in Cloud Computing. *International Journal of Compuetr Science and Information Technologies*, *5*(4), 5825–5827.

Saravanakumar, C., & Arun, C. (2014). An efficient ASCII-BCD based steganography for cloud security using common deployment model. *Journal of Theoretical and Applied Information Technology*, *65*(3), 687–694.

Sarkar, M. K., & Chatterjee, T. (2014). Enhancing Data Storage Security in Cloud Computing Through Steganography. *ACEEE International Journal of Network Security Network Security*, *5*(1), 13–19.

Sarvabhatla, M., M.Giri, & Vorugunti, C. S. (2014). A Secure Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography. *2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*.

Yang, C. L., Hwang, B. N., & Yuan, B. J. C. (2012). Key consideration factors of adopting cloud computing for science. *CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science*, 597–600. https://doi.org/10.1109/CloudCom.2012.6427610

Yang, C., Lin, W., & Liu, M. (2013). A novel triple encryption scheme for hadoop-based cloud data security. *Proceedings - 4th International Conference on Emerging Intelligent Data and Web Technologies, EIDWT 2013*, 437–442. https://doi.org/10.1109/EIDWT.2013.80