ISSN (e): 2250 – 3005 || Volume, 09 || Issue, 4 || April – 2019 ||
International Journal of Computational Engineering Research (IJCER)

Distributed Data Security Enhancement in Public Cloud Storage and Hosting Using Data Obfuscation and Steganograpghy

Momin Uddin, Dr. Shashank Singh
Student,Department of Computer Science and Engineering,Integral University, Lucknow, India.
Assistant Professor,Department of Computer Science and Engineering,Integral University, Lucknow, India.
Corresponding Author; Momin Uddin

ABSTRACT
Cloud computing is based on network and computer applications. In cloud data sharing is an important activity. Small, medium, and big organizations use cloud to store their data in minimum rental cost. At present time, cloud is used by most of the customers because of its services. Therefore, security or privacy of data and data management is to be done properly. In this paper we're going to take the information and distribution it into two distinct part so as to take the security at two levels. At first level, i.e. at hosting site, the image, audio & video files in which the information is encrypted or hidden using steganographic technique. At second level i.e. at cloud,the reference of these files or keys are stored.For data security at cloud, by using steganographic and obfuscation technique where going to address two algorithm, the RSA and DSA algorithms. RSA algorithm can be used for encryption while DSA is used for checking data alteration.
Keywords- *Steganographic, Obfuscation, Cloud, Algorithm, RSA, DSA.*

Date of Submission: 25-04-2019 Date of acceptance:05-05-2019

I. INTRODUCTION

In this synopsis, we are going to take the information and distribute it into two distinct parts so as to make the security at two levels. At first level i.e. at hosting site, the image, audio and video files in which the information is encrypted or hidden using steganographic technique. At second level i.e. at cloud, the reference of these files or keys is stored. Hence, if an attacker might attack, then the reference table or key will be vulnerable & even if he'll get the key but can't do any harm to the main information as he did not know the address of the information where it is stored.

1.1. Cloud Computing

Distributed computing implies that rather than all the PC equipment and programming you're utilizing sitting on your work area, or some place inside your organization's system, it's given to you as an administration by another organization and got to over the Internet, for the most part in a totally consistent manner. Precisely where the equipment and programming is found and how everything functions doesn't make a difference to you, the client—it's only some place up in the shapeless "cloud" that the Internet speaks to.

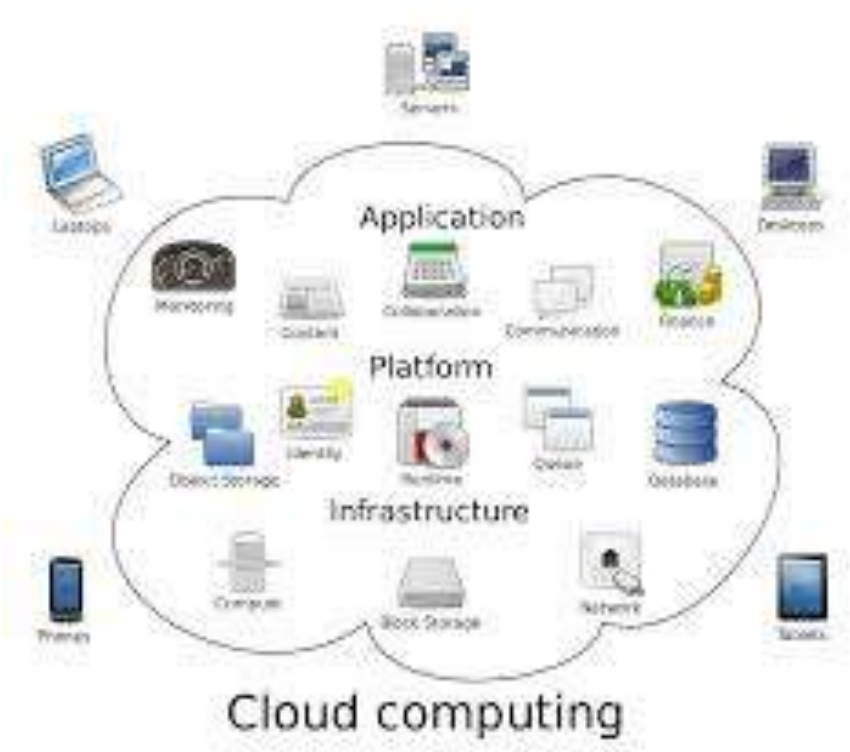

Figure: 1.1

1.1.1. What Makes Cloud Computing Different?

It's managed

In particular, the administration you use is given by another person and oversaw for your sake. In case you're utilizing Google Documents, you don't need to stress over purchasing umpteen licenses for word-handling programming or staying up with the latest. Nor do you need to stress over infections that may influence your PC or about support up the records you make. Google does all that for you. One fundamental standard of distributed computing is that you never again need to stress how the administration you're purchasing is given: with Web-based administrations, you just focus on whatever your activity is and leave the issue of giving trustworthy figuring to another person.

It's "on-demand"

Cloud administrations are accessible on-request and frequently purchased on a "pay-as-you go" or membership premise. So you commonly purchase distributed computing a similar way you'd purchase power, telephone utilities, or Internet access from a service organization. Here and there distributed computing is free or paid-for in different ways (Hotmail is sponsored by publicizing, for instance). Much the same as power, you can purchase to such an extent or as meagre of a distributed computing administration as you need starting with one day then onto the next. That is incredible if your necessities change capriciously: it implies you don't need to purchase your very own huge PC framework and hazard make them stay there doing nothing.

It's public or private

Now we all have PCs on our desks, we're used to having complete control over our computer systems and complete responsibility for them as well. Cloud computing changes all that. It comes in two basic flavours, public and private, which are the cloud equivalents of the Internet and Intranets. Web-based email and free services like the ones Google provides are the most familiar examples of public clouds. The world's biggest online retailer, Amazon, became the world's largest provider of public cloud computing in early 2006. When it found it was using only a fraction of its huge, global, computing power, it started renting out its spare capacity over the Net through a new entity called Amazon Web Services (AWS). Private cloud computing works in much the same way but you access the resources you use through secure network connections, much like an Intranet. Companies such as Amazon also let you use their publicly accessible cloud to make your own secure private cloud, known as a Virtual Private Cloud (VPC), using virtual private network (VPN) connections.

1.1.2. Types Of Cloud Computing

IT individuals talk around three various types of distributed computing, where distinctive administrations are being accommodated you. Note that there's a sure measure of ambiguity about how these things are characterized and some cover between them.

•**Infrastructure as a Service (IaaS)** implies you're purchasing access to crude figuring equipment over the Net, for example, servers or capacity. Since you purchase what you need and pay-as-you-go, this is frequently alluded to as utility figuring. Conventional web facilitating is a straightforward case of IaaS: you pay a month to month membership or a for each megabyte/gigabyte expense to have a facilitating organization present records for your site from their servers.
•**Software as a Service (SaaS)** implies you utilize a total application running on another person's framework. Electronic email and Google Documents are maybe the best-known precedents. Zoho is another outstanding SaaS supplier offering an assortment of office applications on the web.
•**Platform as a Service (PaaS)** implies you create applications utilizing Web-put together instruments so they keep running with respect to frameworks programming and equipment given by another organization. Along these lines, for instance, you may build up your very own web based business site yet have the entire thing, including the shopping basket, checkout, and installment instrument running on a trader's server. Application Cloud (from salesforce.com) and the Google App Engine are instances of PaaS.

Advantages and disadvantages of cloud computing
Advantages
The geniuses of distributed computing are clear and convincing. In the event that your business is selling books or fixing shoes, why get engaged with the low down of purchasing and keeping up a mind boggling PC framework? In the event that you run a protection office, do you truly need your business operators dawdling running enemy of infection programming, overhauling word-processors, or agonizing over hard-drive crashes? Do you truly need them jumbling your costly PCs with their own messages, illicitly shared MP3 records, and devious YouTube recordings—when you could leave that duty to another person? Distributed computing enables you to purchase in just the administrations you need, when you need them, cutting the forthright capital expenses of PCs and peripherals. You maintain a strategic distance from gear leaving date and other well-known IT issues like guaranteeing framework security and unwavering quality. You can include additional administrations (or remove them) immediately as your business needs change. It's actually snappy and simple to add new applications or administrations to your business without hanging tight weeks or months for the new PC (and its product) to arrive.

Disadvantages
Moment comfort includes some significant pitfalls. Rather than buying PCs and programming, distributed computing implies you purchase administrations, so one-off, forthright capital costs become progressing working expenses. That may work out substantially more costly in the long haul.

1.1.3. Steganography

The word steganography originates from the Greek Steganos, which mean secured or mystery and graphy mean composition or drawing. Consequently, steganography implies, actually, secured composing. The principle objective of steganography is to convey safely in a totally imperceptible way and to abstain from attracting doubt to the transmission of a concealed information.There has been a fast development of enthusiasm for steganography for two primary reasons: The distributing and broadcasting businesses have turned out to be keen on strategies for covering up encoded copyright imprints and sequential numbers in advanced movies, sound chronicles, books and sight and sound items. Moves by different governments to confine the accessibility of encryption administrations have propelled individuals to contemplate strategies by which private messages can be installed in apparently harmless spread messages.

Steganography Pros
- One-Way Hashing
- Attaching Text to an Image
- Hiding Information

Steganography Cons
- Shockingly most employments of steganography and research around the theme of steganography revolve around the ill-conceived purposes. The three greatest territories of ill-conceived steganography advance around psychological warfare, sex entertainment and information robbery.

- Distributed computing might be a use of registering assets that is conveyed as an administration over a system, the administration might be an equipment or programming. Cloud overpowers it industry by its huge qualities. As indicated by NIST-
- Distributed computing is a model for empowering omnipresent, accommodating, on-request arrange get to a common pool of configurable processing assets that can be immediately provisioned and released with insignificant organization effort or advantage supplier communication.
- Cloud gives three kinds of administrations like Infrastructure as a Service (IaaS), Program as a Service (SaaS) and Platform as a Service (PaaS). IaaS could be an administration display that conveys gear, limit, servers and data focus to the customers. A standout amongst the most organizations given by the cloud is Storage as A Service (StaaS).
- Privacy of data is to be ensured by cryptography, confusion and steganography methodology.
- Cryptography is a powerful technique that has any kind of effect to guarantee the data from unapproved get to while data very still in cloud server. Cryptography is a strategy for securing and transmitting data in a particular edge so that in a manner of speaking those for whom it is expecting can look at and handle it. It is the strategy for encryption and deciphering.
- Cryptographic strategies are arranged into Conventional and Public key Cryptography. Traditional Cryptography is moreover insinuated as symmetric key cryptography. A similar key is used for encryption and decoding in symmetric key cryptography.

1.1.4. Obfuscation

Obfuscation is the method of hiding the original value of data. It is a process applied to data to intentioned make it troublesome to invert without knowing the algorithm that was connected. The most distinction handled without the key required for decryption. So also, jumped information can be handled without any requirement of key.

Data Obfuscation (DO) is a type of information veiling where information is intentionally mixed to avert unapproved access to touchy materials. This type of encryption results in incomprehensible or confounding information. There are two sorts of DO encryption:

1.Cryptographic DO: Input information encoding before being exchanged to another encryption diagram.

2.Network security DO: Payload assault strategies are intentionally enrolled to stay away from recognition by system insurance frameworks.

DO is otherwise called information scrambling and security protection.

II. LITERATURE REVIEW

In paper [1], these days giving and keeping up the security and trustworthiness of the information while it is exchanged through open channels is an extreme undertaking. To conquer this test the author gives a strategy to verify the information through picture steganography. It is an altered LSB picture steganography method which utilizes secret phrase to shroud the information in a picture. For concealing the information a following technique is followed in which good for nothing code are produced and the coordinating depends on secret word coordinating. In this paper, three strategies are broke down to spare the good for nothing code: Method 1, Method 2, and Method 3. In Method 1, high pinnacle flag to commotion proportion esteems which are acquired. In technique 2 and 3 both have crest flag to commotion proportion esteems which are tantamount yet the Method 3 is controlled and is reliant on the situations in number of bits to store.

In paper [2], the author centers around making a protected cloud biological system wherein we utilize multifaceted verification alongside different dimensions of hashing and encryption. Alongside the recreated outcomes. The calculation portrays the working of the framework by speaking to the whole procedure from client validation to capacity and recovery of client information from cloud. This paper exhibits a mixture cryptography framework that joins the advantages of both symmetric and lopsided encryption. Secure cloud biological community is proposed to guarantee information security and protection by actualizing diverse encryption procedures at different dimensions. The framework additionally utilizes certain hashing and salting procedures which even quality the whole encryption process, likewise ensure believed verification along these lines permitting the component of one time password, and wish to join clear advances that would upgrade the proficiency and simplification of our frameworks.

In papers [3], the author considered applying two steganographic recommendations (steghash and socialsteghash) for another appropriated correspondence framework by satisfying presumption for cyberfog security approach. Another idea of the conveying framework understanding the possibility of cyberfog security was displayed the plan consolidates and adjusts a couple of segments, for example, steghash for ordering information. Socialstegdisc for filesystem activities and trustMASS for gadget to gadget information transmission. Security is portrayed by the way that the halfway trading off of the framework does not interface the activities, while caught tests are pointless for the foe.

In paper [4], the author gives another cloud security and protection display (CSPM) into layer which can be considered by cloud supplier amid every one of the phases of the cloud administrations building and observing. This model will allow to defeat this cloud administrations boundary selection and in this way, to assemble trust in cloud administrations and furthermore to give secure administrations. At last, we will show some security dangers and assaults, and propose, as per CSPM, a few countermeasures. Procedures must be improved or changed to work viably with the cloud nature so as to guarantee an abnormal state of access security to cloud administrations from few assaults like record and administration commandeering assaults. These security of information and access control and benefit the board layers of CSPM. To be sure cloud condition is broadly circulated, exceedingly unique and increasingly undermined by assaults. Hence, these countermeasures must be improved or changed to work successfully in this kinds of condition.

In paper [5], the author centers around how to build a PEKS diagram by means of obscurity. The fundamental plan is based on the Differing-Inputs Obfuscation (DIO) and can be considered as an underlying endeavor to apply DIO in the PEKS field. In this paper, the author centers around how to develop an open key encryption with catchphrase seek conspire (PEKS) by means of muddling. To our joy, we find that DIO can be utilized to manufacture PEKS plans. Applying contrasting sources of info confusion in PEKS field and get a few intriguing hypothetical outcomes. This paper exhibits an essential PEKS plot supporting single catchphrase look which can be effectively reached out to help complex functionalities and to that in the multi client setting. We consider the KGA security of PEKS and improve our essential plan to oppose disconnected watchword speculating assaults. Contrasted and PEKS plans opposing KGA assaults, this plan is a standard one instead of a PEKS conspire with an assigned analyzer. The confinement of this plan is self-evident, i.e, the trapdoor created process is wasteful which may make them inapplicable in asset restricted conditions. Disdain of the outcomes gotten by applying muddling in PEKS development, it must be brought up that these PEKS plans neglect to confirm the accuracy and culmination of the query item from the server.

In paper [6], the fundamental purpose behind this move is a result of the various advantages given by cloud benefits over the system. Information recuperation is the one of the vital idea while managing capacity gadget which are essentially the foundation of the cloud framework. In this paper, the author investigate the security issue which can be arised dependent on the utilization of information recuperation apparatuses on cloud framework, when the client have erased their information. To address this issue, the author proposed a straightforward strategy utilizing rename. To address the security issues related with the information recuperation and ensure the client information in the cloud after cancellation, author proposes a straightforward system in the cloud to tackle the recuperation issue and making hard for unintended recuperation of private client information after erasure. Propose structure comprise of another module (rename) for changing the expansion of the records contrasted with general cloud engineering. In this work author talked about the structure to verify the information utilizing information recuperation apparatuses or procedures. Likewise, a basic structure is proposed to secure the client information in the cloud. The proposed structure works successfully by utilizing the idea of record positions it will be difficult to comprehend the substance of the documents in wrong information group except if these document are altered to unique information designs.

In paper [7], the author had presented a vigorous strategy for vague sound information stowing away. Along these lines we reason that sound information concealing methods can be utilized for various purposes other than clandestine correspondence or deniable information stockpiling, data following and finger printing, alter recognition. As the sky isn't constrain so isn't for the improvement. Man is presently pushing without end its very own limits to make all musings imaginable. So likewise these activities depicted above can be additionally altered all things considered in the realm of Information Technology Data transmission in open correspondence framework isn't verify a direct result of block attempt and inappropriate control by meddler. So the alluring answer for this issue is Steganography, which is the craftsmanship and exploration of composing shrouded messages so that nobody, aside from the sender and expect beneficiary, associates the presence with the message, a type of security through lack of definition. Sound steganography is the plan of concealing the presence of mystery data by disguising it into another medium, for example, sound document. In this paper we primarily examine distinctive kinds of sound steganographic techniques, preferences and burdens.

In paper [8], the author dissected the different security viewpoints that are helpless against the distributed computing and should have been settled. Different dangers from system level to application level are probably going to occur in distributed computing and these should be checked in order to make our cloud increasingly secure. Privacy and honesty of information ought to be kept up with the goal that the information stays secure. It additionally discloses to us the different targets that will improve the security of information in cloud. Real enhancements should be done in transfer speed that is required to send information over system and increment the limit of the cloud to hold information.

In paper [9], the author proposes an information muddling approach in redistributing lattice increase to cloud part. Fundamentally dependent on part the lines and segments of lattices to modify their real measurement combined with including arbitrary commotion and rearranging so as to guarantee secrecy and security. Muddled

lattices are send to server with no open key encryption. While it processes on lattices the server is unfit to extricate or get real qualities either from muddled networks or from figured increase results. While, customer can separate genuine figured qualities utilizing an inconsequential processing exertion from results delivered by the server. The customer is required to spend an irrelevant exertion to part the grids. It would not cost more than O(n). the customer can register the way toward part their mstrices utilizing hand-held low fueled gadgets. This strategy does not require any encryption so that, the cloud server does just framework duplications, and does not required any extra calculation because of part of lattices, acquainting clamor with qualities and rearranging of lines utilizing information jumbling procedure in re-appropriating processing to cloud seems progressively practical and secure for the customer. We are at present attempting to contrast our methodology and other comparable strategies, specifically, the computational execution of the recuperation procedure. moreover, we intend to reproduce the methodology with substantial informational collections in a genuine distributed computing setting.

In paper [10], the author audited diverse steganography procedures for scrambling the information. Steganography is a system that enables the one to shroud the information inside a picture while including couple of perceptible changes. This paper examines the idea driving the steganography by investigating right off the bat what is the steganography and the terms that are identified with steganography. This paper investigates the steganography techniques – picture steganography, sound steganography, video steganography, content steganography that are utilized to implant the data in computerized transporters. The two most imperative parts of picture based steganography framework are the nature of stego picture and the limit of the spread picture. By assessing this paper, analysts can build up a superior steganography system to expand the MHC and PSNR esteem by examining the current steganalysis procedures. In the previous couple of years, the steganography is intrigued point for picture spread media. This paper give a review of steganography and present a few systems of steganography which help to install the data. These procedures are progressively valuable for identifying the stego pictures just as the picture media identifying with security of pictures and insert the information for complex picture zone and you can undoubtedly appraise the high implanting rate by utilizing the quantitative steganalytic strategy.

In paper [11], the author portrays a multilayer security framework called "Application Protected Execution"(APEx) that has a " In-VM observing" usefulness ensured by out-of-band memory made inside a virtual machine on cloud based hubs. The paper additionally portrays an application that employes APEx to shield client space programming from figuring out and return situated programming (ROP) assaults. The application "Code Obfuscation Engine" (CObe) perform code mixing and uses framework gets and out-of-band memory to obscurity program stream and return the stack. Using APEx, it can hop into out-of-band memory for execution of delicate code territories, figuring of bounce focuses and return addresses. This ensure programs stream against high jacking-particulary support flood and ROP assaults. CObe changes a double record for use with APEx secured execution legitimately and does not require source code. The outcomes are very encouraguing for the execution angles for the self-obscurity applications. notwithstanding for execution basic application with restricted registered assets, there are a lot of tasks that can be used bringing about effect to execution. Notwithstanding for the outrageous case incidental emplacement of MS administrators for hardenimg the obscurity should be possible at key purposes of the code for insignificant by and large effect. This paper concentrated on the plan and execution of the out-of-band GSIM layer and the code obscurity, code mixing, and code concealing utilizing the GSIM layer.

In paper [12], the author proposed a technique to portray how to verify information and data in cloud as far as information sharing or putting away. The author utilizes cryptography and steganography systems to verify the information in cloud. Here, RSA calculation is utilized with some other calculation to give greater security. By testing this technique, a more grounded structure for security of information in distributed computing is created. A superior security of information in cloud is given. The working of these calculations must be improved as far as vigor and concealing ability to make it increasingly secure.

In paper [13], the author proposed another calculation to verify steganographic document which is imperceptible by bits correlation apparatus and some other strategy. This calculation, which utilizes those bits of picture RGB and LSB values which are same as the estimation of message to be covered up. Pictures are send in the beginning by physical methods after that picture number and recipe is moved in hash structure. This procedure makes the hundred percent secure correspondences. In this paper, two calculations are utilized for steganographic document making. First is encryption calculation and the second is unscrambling calculation. This calculation is hundred percent secure as we are not sending even a solitary piece of mystery message over the system. Utilizing two phases, first to move cluster in hash structure with pixel areas of picture whose bit qualities to be picked to recover the message and also to exchange pictures either by physical transportation or online with some hole is a hundered percent secure system by which security can be practiced in exchanging information over the system. We pick case one for exchange of picture as done amid key trade innovation of key based cryptographic methods the mystery message can't be gotten by any gatecrasher using any and all means.

Security objective like privacy and trustworthiness of message exchanged over system. Another calculation to verify picture steganographic record is additionally proposed which can verify information totally.

In paper [14], to address the issue of both cloud client just as specialist co-op, we proposed another plan by putting encryption and obscurity procedure cooperates. Information will be scrambled before sending on cloud server dependent on affectability of information and client stayed quiet offers security to information experiencing significant change. Indeed, even key isn't imparted to any one and information accessible in encoded group on cloud machine influences client to guarantee about classification. We utilized obscurity system for security reason at cloud server side by which there is less possibility of hardening the information. We proposed a calculation which bolsters this tasks and giving that client driven and server driven control together which give satisfactory security benefits like by actualizing bunch sharing approach from the model investigation it is seen that proposed plan gives better insurance to put away data on a cloud than the current procedures which depend on encryption,onfuscation method alone from cloud clients too specialist organizations see.

In paper [15], a picture assurance technique is proposed to guarantee computerized picture security and protection over the cloud framework. We utilize the steganography procedure to cover the luminance just as the sub sampled chroma parts of a private picture. The proposed strategy can cover a private shading picture, unlawful programmers and assailants won't perceive the presence of private pictures even they barged in wildly into the distributed storage. Besides, the proposed technique can decrease the span of the picture documents and increment the distributed storage limit.

III. CONCLUSION

From the above papers that I have reviewed are secured in various ways using different algorithms. But those strategies and algorithms provides the security of data only at cloud which might be retrieved by an attacker. So I have proposed a method in which we distribute the data into two parts i.e. at the hosting site and at cloud. At hosting site, we're going to store images, audio and video files which are encrypted using steganographic method. At cloud, the reference of the images, audio and video files or their keys are stored. So, even if someone got the key or reference from the cloud then he/she cannot get the information as the other half encrypt file is present somewhere.

REFERENCES

[1]. Akshay, K. C., & Muniyal, B. (2018, September). Analysis of Data Hiding Methods in Image Steganography. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 2023-2027). IEEE.

[2]. Arora, A., Khanna, A., Rastogi, A., & Agarwal, A. (2017, January). Cloud security ecosystem for data security and privacy. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 288-292). IEEE.

[3]. Bieniasz, J., & Szczypiorski, K. (2018, September). Towards Empowering Cyber Attack Resiliency Using Steganography. In 2018 4th International Conference on Frontiers of Signal Processing (ICFSP) (pp. 24-28). IEEE.

[4]. El Makkaoui, K., Ezzati, A., Beni-Hssane, A., & Motamed, C. (2016, May). Cloud security and privacy model for providing secure cloud services. In 2016 2nd international conference on cloud computing technologies and applications (CloudTech) (pp. 81-86). IEEE.

[5]. Hu, C., Liu, P., Yang, R., & Xu, Y. (2019). Public-Key Encryption With Keyword Search via Obfuscation. IEEE Access, 7, 37394-37405.

[6]. J. Surbiryala and C. Rong, "Data Recovery and Security in Cloud," 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA), Zakynthos, Greece, 2018, pp. 1-5.doi: 10.1109/ IISA.2018.8633640

[7]. Jayaram, P., Ranganatha, H. R., & Anupama, H. S. (2011). Information hiding using audio steganography–a survey. The International Journal of Multimedia & Its Applications (IJMA) Vol, 3, 86-96.

[8]. Kajal, N., & Ikram, N. (2015, May). Security threats in cloud computing. In International Conference on Computing, Communication & Automation (pp. 691-694). IEEE.

[9]. Khan, K. M., & Shaheen, M. (2015, August). Data Obfuscation for Privacy and Confidentiality in Cloud Computing. In 2015 IEEE International Conference on Software Quality, Reliability and Security-Companion (pp. 195-196). IEEE.

[10]. Mahajan, S., & Singh, A. (2012). A Review of Methods and Approach for Secure Stegnography. International Journal of Advanced Research in Computer Science and Software Engineering, 2(10).

[11]. Mumme, D. C., Wallace, B., & McGraw, R. (2017, June). Cloud Security via Virtualized Out-of-Band Execution and Obfuscation. In 2017 IEEE 10th International Conference on Cloud Computing (CLOUD) (pp. 286-293). IEEE

[12]. Pant, V. K., Prakash, J., & Asthana, A. (2015, October). Three step data security model for cloud computing based on RSA and steganography. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 490-494). IEEE.

[13]. Sharma, A., Sharma, N., & Kumar, A. (2017, January). A new algorithm to secure image steganographic file. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 570-573). IEEE.

[14]. Suthar, K., & Patel, J. (2015, November). EncryScation: A novel framework for cloud iaas, daas security using encryption and obfuscation techniques. In 2015 5th Nirma University International Conference on Engineering (NUiCONE) (pp. 1-5). IEEE.

[15]. Wu, W. C., & Yang, S. C. (2017, June). Enhancing image security and privacy in cloud system using steganography. In 2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW) (pp. 321-322). IEEE.

Momin Uddin" Distributed Data Security Enhancement in Public Cloud Storage and Hosting Using Data Obfuscation and Steganograpghy" International Journal of Computational Engineering Research (IJCER), vol. 09, no. 4, 2019, pp 31-37