IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 2 ISSUE : 1 Print / Issue Publication Date: 31-Dec-2016

ISSN : 2455-2143

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 44-48
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

REVIEW PAPER ON ENHANCING DATA SECURITY FOR CLOUD ENVIRONMENT CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUE

Deepika
Research Scholar (CSE)
S.S.C.E.T, Badhani
Pathankot, India

Gurjeet Kaur
Assistant Professor (CSE)
S.S.C.E.T, Badhani
Pathankot, India

***Abstract*— The Cloud Computing is a dynamic term, which provides dispute free data outsourcing facility which prevent the user from burdens of local storage issues. However, security is perceived as a biggest issue and poses new challenges related to providing secure and reliable data archive over unreliable service providers. In this paper, we proposed a novel method to enhance security aspects by associating cryptographic techniques along with Steganography.**

Keywords— **Cloud Computing, Security, Cryptography, Steganography, AES.**

I. INTRODUCTION

Cloud computing is the name stated to the latter trend in computing service provision. With this trend the way of computing has gone for a sea change. Cloud computing is an emerging paradigm in the field of Information Technology. Cloud refers to widespread internet which means cloud computing is an internet based computing where services are delivered to users via internet. Capabilities such as processing, storage and other capabilities are now provided on-demand, as a service and both freely and at cost [1]. It provides an efficient, convenient, transparent method of procuring/obtaining IT services such as Infrastructure, Software, and Platform that offers many benefits including flexibility, efficiency at a nominal reduced cost via outright procurement. Earlier days when data was accommodated under consumers own security and administrative domain, has now been extracted and placed under the domain of the Cloud Service Provider (CSP) [2]. However, cloud computing has to face several challenges/issues. As more and more data of an individual or companies are placed in the cloud, so as concerns are beginning to grow that how much safe this environment is. Despite of all the hype surrounding the cloud, companies and Individuals are still reluctant to place their data on to the cloud. Security and privacy is one of the major concerns which is one of the barriers in the growth of cloud computing and when data is out of the boundaries of an organization these concerns raise it-self. Organizations have been able to collect huge amount of private information of an individual. To attenuate these concerns, a cloud vendor must assure that clients can continue to have the similar privacy and security controls over their applications, for they are the ones who will shoulder the responsibility if things go wrong [3].

Cloud Computing is not completely perfect, because there are many aspects that are needed to be worked out like security issues. There are various key factors which are describing that why cloud computing is popular among several organizations.

a) **Preserve Productivity**: By permitting numerous clients to take a shot at same archive progressively spares much measure of time and upgrade the business profitability. Besides, same environment for preparing numerous solicitations diminish the twofold work and endeavors.

b) **Reliability**: The motivation behind why distributed computing is mushrooming is their colossal unwavering quality element. Distributed computing offers host of business and association from all aspects of the world.

c) **Save cash**: Users of cloud just need to pay as indicated by their assets use. It depends on 'pay as you go' run the show. Clients don't need to pay extra assets which the not utilize. In this way, this is the excellence of distributed computing.

d) **Elastic Resources**: We can without much of a stretch scale up and downsize the assets from cloud stage.

A. Security Challenge in cloud computing

As cloud computing helps associations to hone their development and execution. Other than this, it likewise has numerous clients to give access to imparted assets to less exertion. In any case, security issues or dangers are still a hindrance in the achievement way of distributed computing. Quantities of reasons are the matter. In the first place reason is that clients and numerous associations store their information on distributed storage, so the essential concentration is the information must be secure, and the information are not being lost and altered while heading out starting with one place then onto the next over the system. So it is basic that privacy, accessibility and uprightness of

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 44-48
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

information ought to be guaranteed. Besides, unapproved get to where an aggressor tries to be the impersonator of the lawful client. [3]

Security Issues at various layers in cloud computing

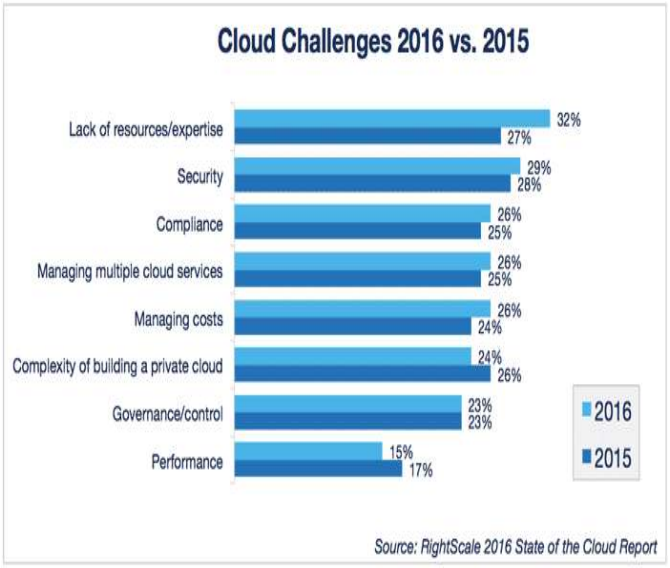


Fig 1.Security Challenge in cloud computing

In cloud computing each layer is associated with different security problems. These security concerns are ranked based on the different layers of the cloud infrastructure namely; application level, network level, level of data storage, virtualization level, authentication and access control level.

1. Application level security issues

Risks at the application level directly affect the cloud applications at a user level. However, the application layer contains the key issues that are on the service availability and integrity of the state of workload. Solutions supplied to lessen these kinds of issues are the encryption techniques and DDoS detection methods to prevent DOS attacks.

2. Network level security issues

Interconnection network cloud should be reasonable. But there are certain general network attacks that occur to access cloud services. These attacks are DNS poisoning attacks, phishing attacks, IP spoofing attack.

3. Data storage level security issues

Data storage level includes various challenges:

a) **Data-in-Transit**- This challenge mainly affects the confidentiality and integrity of data due to poor encryption mechanisms and network protocols.

b) **Data loss**- Cloud users using storage services for their personnel data can be lost if hacker attacks to main storage service.

c) **Data location**- Essentially, following the area of client information is troublesome in the cloud until the client information are progressively relocate starting with one area then onto the next area. Emerges the issue of information protection and security and the client can control the loss of its information..

d) **Data integrity**- In public cloud, where information can be gotten to anyplace and at whatever time postures hazards as anybody can get to other information and making alterations to it, which influence the integrity of the information.

4. Virtualization level security-

In the multi-tenant environment, multiple virtual machines that have their own operating system running simultaneously on a single physical platform (host computer), it means that multiple guest operating system running on hyper visor increases security risks in case if the guest operating system to run malicious code to accommodate the machine to have full access to the physical machine, including other guest virtual machines. This type of risk generates either a collapse of the system or loss of data. The attacks have been found mainly in the virtual layer is the blue pill, Sub Virt..

5. Authentication and authorization level security issues

In problems of authentication and authorization level security, risks that have participated include unauthorized access. Password capture attacks are serious threats to authentication level. It includes threats of keyboard loggers, screen scrapers, dictionary attacks and data attacks shoulder surfing. Therefore, a strong authentication mechanism is required to verify legitimate users and to keep out hackers. [11]. The ultimate objective of preserving privacy is to minimize the risk of misuse of data and simultaneously produce results that are similar to the results produced when such privacy preserving techniques are not implemented.

II. RELATED WORK

1) A reliable data protection model based on re-encryption concepts in cloud environments", Moghaddam F. F, Vala M, Ahmadi M, Khodadadi T, and Madadipouya K [2015]

This paper [1] presents a hybrid encryption model using classification indexing, attributes and time based procedures. Data classification is mainly based on attributes. A hybrid ring was used to establish the security between the rings. These securely protected rings perform the re-encryption in order to protect themselves from un-authorized access, time based, data owner request and user revocation. The result analysis shows that the hybrid ring model enhances the reliability and the efficiency of the data protection applications.

2) "An improved LSB based image steganography technique for RGB images", Singh Amritpal and Singh H, [2015]

This paper [3] proposed an enhanced LSB based Steganography procedure for images bestowing better data security. It exhibits an embedding algorithm for hiding ciphered messages in nonadjacent and irregular pixel areas in edges and smooth regions of images. The edges in the cover-image are detected using improved edge detection filter. The encrypted message bits are then embedded in the least significant byte of randomly selected edge pixels and some specific LSBs of red, green, blue components respectively. Such type of steganography technique ensures least chances of suspicion about message bits hidden in the image and it gets hard to estimate the true message length by standard steganography detection methods. The Proposed approach shows better results in PSNR value and Capacity as compared to other existing techniques.

3) **"Graphical Password Authentication", Prathamey K. Rane,Leena S. Gawade[2014]** describes all graphical methods for password authentication system and also proposed an approach which describes that first calculation has been done by server based on user entered username and according to result one set of images will be transferred on user screen, each set contains hundreds of images, and then user has to select two images from given set, whereas server also add two images by its own to form complete password.

4) **"Efficient integrity verification of replicated data in cloud using homomorphic encryption", Raghul Mukundan, Sanjay Madria, Mark Linderman[2014]**

In this paper cloud service provider (CSP) is aid for information proprietors, to outsourcing their information and decrease their weight of neighborhood information stockpiling and upkeep. Cloud benefit supplier repeats the information to build the information accessibility, unwavering quality and strength. What's more, customers or information proprietors need to pay to store information to CSPs stockpiling place. To keep up the information classification stops the cloud benefit supplier from tricking by keeping up less duplicates than paid for information, in this paper they propose the Dynamic Multi Replica Provable Data Possession plot (DMR-PDP). This plan additionally gives administration of element operations with the end goal that inclusion, cancellation and alteration on recreated information over the cloud server.

5) "A Trust Based Approach for increasing Security in Cloud Computing Infrastructure", Hamid Banirostam and Alireza Hedayati [2013] One new approach is characterized named Trusted Cloud Computing Infrastructure (TCCI) which depends on Infrastructure security. TCCI approach portrays that diverse hubs are required to keep running on secure environment so to keep programmers away. In addition, if hub keeps running in a safe domain than even executive is unequipped for get to the client information. To make the framework secure TCCI approach is proposed which handles the hubs by outsider known as Trusted Coordinator (TC).

6) **"A strengthening plan for enterprise information security based on cloud computing", An Na Kang, Lard Brollie, Jong Hyug Park, Young-Sik Jeong[2013]**

cloud computing is most broadly utilized administration that gives an assortment of processing assets, from servers and capacity to big business applications like email, security and reinforcement all conveyed over the web. cloud computing deals with the client's IT assets and in addition undertakings the IT assets in a compelling way. With the improvement of web cloud computing successfully oversee and utilize the quantity of information. While utilizing cloud computing such a large number of dangers have happened, since they will ascend to security dangers to big business data. As a result of the quality endeavor broadly utilize the cloud computing. Confirmation and get to power administration is the essential thought to be considered to ensure data spillage, benefit deliberation and so on. Center elements that cloud computing use to secure information are administration of keys and effective encoding.

III. PROPOSED WORK

3.1 Problem Formulation

Cloud computing is growing vastly by providing various functions such as global resource scheduling, fault tolerance, reliability and load balancing. As discussed in chapter 2, it shows that cloud security is still a barrier to adoption of this service. Cloud Security incorporates many security restrictions from the point of view of the customer and cloud providers. In the context of customers, who essentially concerned about that;

- Where data is stored?
- Who has the right to see their data?

With regards to cloud suppliers, they additionally confront challenges in meeting the Cloud Security Organization together indicated by clients and to meet their own administration destinations unsurprising increase (pick up or benefit). Numerous hypotheses and methods have been actualized to adapt the security issues. Upgrades in encryption systems have been seen to lessen the information security dangers. Yet, many dangers at the verification level in cloud computing are still need to determine. Cloud clients store their information on cloud storage and they require not to stress over space contemplations, purchasing new capacity hardware or deal with their information, they just need to get to their information whenever from wherever the length of they have web get to. Be that as it may, because of numerous security issues it stopped the associations to interface with cloud computing totally. One of the primary disservices of cloud computing is its gigantic security dangers. In this study different security parts of security issues has been broke down and afterward proposes a structure to relieve security issues at the level verification and capacity level in cloud computing. Productive security components ought to be sent by method for encryption, verification, and approval or by some other strategy to

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 44-48
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

guarantee the protection of shopper's information on cloud storage.

a) Confidentiality: This incorporates two primary ideas: Data Confidentiality which alludes that staff or private data of client in cloud should not be unveiled to unapproved client. Security alludes individual control implies what data is gathered and who can see this data.

b) Integrity: A loss of integrity means complete loss of unique of data. Moreover, integrity can be an information integrity and system integrity

c) **Availability:** It says that reliable and timely access is important factor. However, a loss of availability means the loss of data access.

3.2 Objectives: The objectives of our proposed work are to implement a secure cloud system using cloud sim simulator. Enhance the authentication security of the cloud computing using image sequencing passwords. We have Increase the confidentiality and security of the cloud computing through hybrid security preserving technique. To ensure the integrity of the data using Hash codes To compare the results of proposed technique with the existing techniques on the basis of:

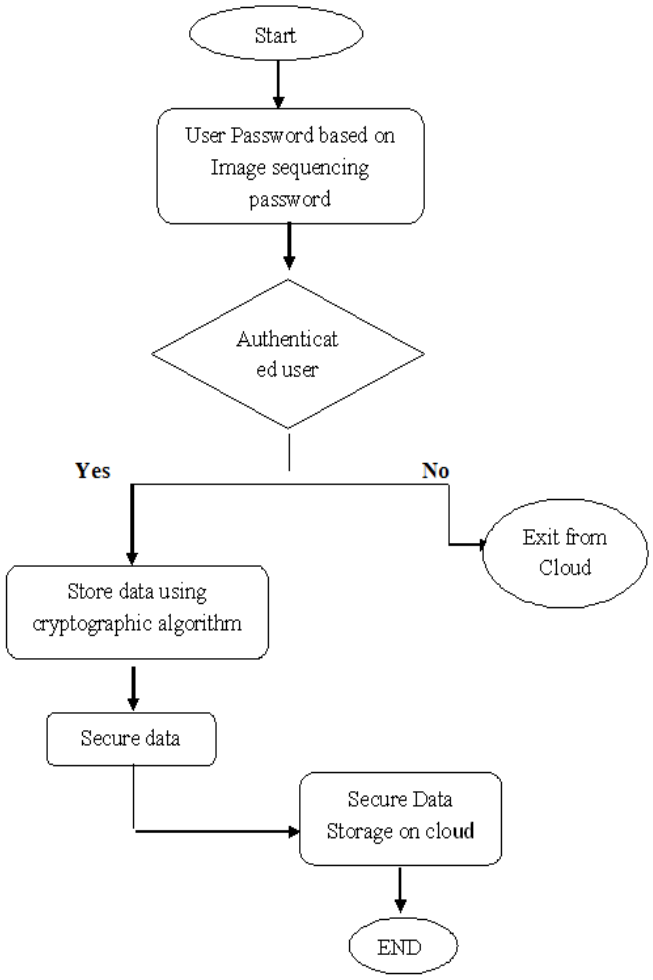
a. Data Encryption time
b. Data Decryption time

3.3 Methodology

To solve the problem of security in cloud computing, we are going to deploy these two-way techniques for preventing security breaches on cloud computing. One is image sequence base password provides security from authentication attacks at user end. Cryptographic Algorithm use for secure encryption of data over our cloud.

1. **Image Sequencing Password:** This password is based on the sequences of some images. It is much secure because sequence of images is change every time. Basically, this password is use for authentication purpose. Only legitimate user will allow entering in cloud, if they enter the correct sequence of image. After authentication, during access of data operations this interface will again ask the user sequence, this time images gets shuffle, based on sequence of images password will also be change.
2. **Cryptography algorithm:** To keep the data secure from attackers on the network, data is hidden inside the image using randomized and anonymized privacy preserving techniques embedded in steganography technique. Then sending that pixel's data file to the cloud environment.

a) Image as an input and apply canny edge detection algorithm to find edges
b) Dataset and convert it into binary form.
c) Store those edges and their positions in an array and **randomly select one index of that array**; then check the Lsb if Lsb is 0 and message bit also 0 then use that Lsb otherwise again select the next array index randomly.
d) **Store the array index which are used for message hiding into a text file and send that file to cloud** and store that array containing edges and their positions at the local end.
e) For Decryption, **select that text file which is sent to cloud and match its array index with the array which is stored at the local end** and decrypt the message from its Lsb.



3.5 Tool Used For Simulation

The proposed methodology is should have been executed in a device. The proposed arrangement is to be executed in java and Cloud Sim. Cloud Sim empowers displaying, recreation, and investigating Cloud computing foundations. It is an independent stage used to model server farms, benefit agents, booking and distribution approaches of huge scale Cloud stages. It furnishes a virtualization motor with broad elements for demonstrating creation and life cycle administration of virtual machines in a server farm, including strategies for provisioning of virtual machines to hosts, planning of assets of hosts among virtual machines, booking of undertakings in virtual machines, and displaying of costs bringing about in such operations.

IV. CONCLUSION

Cloud Computing is envisaged as the next unruly wave. But besides its advantages, preserving privacy is one of the major issues that become a barrier in the growth of Cloud Computing. One of the most popular techniques of security preserving technique was used in Cloud Computing to preserve privacy but none of the techniques addresses the issues properly. Hence, the key conclusion of this thesis is that, a technique called secure technique in Cloud Computing Environment has been proposed which aims to provide privacy without any loss of information. By this the sensitive information of individual remains preserve. As in this technique randomly generated index values corresponds to the pixel values of picked image is sent on the cloud instead of actual data therefore it becomes very difficult to restore actual data without recognising that what these bits and bytes actually point to.

V. REFERENCES

[1] F. F. Moghaddam, M. Vala, M. Ahmadi, T. Khodadadi, and K. Madadipouya, "A reliable data protection model based on re-encryption concepts in cloud environments," 2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC), pp. 11–16, 2015.

[2] A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1–4, 2015.

[3] S. M. Gurav, L. S. Gawade, P. K. Rane, and N. R. Khochare, "Graphical password authentication: Cloud securing scheme," 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies, pp. 479–483, 2014.

[4] Mukundan, R.; Madria, S.; Linderman, M. (2014) "Efficient integrity verification of replicated data in cloud using homomorphic encryption", Springer Distributed and Parallel Database, vol. 32, Issue 4, pp. 507-534, 24 June 2014

[5] Banirostam h., & Hedayati, A. (2013) "A Trust Based Approach for increasing Security in Cloud Computing Infrastructure" International Conference on computer modeling and simulation, IEEE, Cambridge, pp. 717-721.

[6] Kang, A.N.; Barolli, L.; Park, J.H.; Jeong, Y.S. (2013) "A strengthening plan for enterprise information security based on cloud computing", Springer cluster computing, vol. 17, Issue 3, pp. 703-710, September 2013

[7] Du, Y.; Zhang, R.; Li, M. (2013) "Research on security mechanism for cloud computing based on virtualization" Springer Telecommunication systems, Vol. 53, Issue 1, pp. 19-24, 2013

[8] Chen, D., & Zhao, H. (2012). "Data Security and Privacy Protection in cloud computing." 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), pp. 647-651,2012.

[9] Abuhussein, A., Bedi, H., & Shiva, S. (2012) "Evaluating Security and Privacy in Cloud Computing Services: A Stakeholder's Perspective", 2012 International Conference for Internet Technology and Secured Transactions, pp.388-395,2012.

[10] M.-H. M. Guo, H.-T. H. Liaw, L.-L. Hsiao, C.-Y. Huang, and C.-T. Yen, "Authentication using graphical password in cloud," 2012 15th International Symposium on Wireless Personal Multimedia Communications (WPMC), pp. 177–181, 2012.

[11] Usha, S., Kumar, G. A. S., and Boopathy bagan, K., A secure triple level encryption method using cryptography and steganography, Computer Science and Network Technology(ICCSNT), International Conference, pp. 1017-1020,2011.

[12] Marwaha, P., Visual cryptographic steganography in images, Communication and Networking Technologies(ICCCNT), International Conference, pp 1-6, 2010

[13] Umamaheswari, M., Siva Subramanian, S. and S. Pandia rajan S., Analysis of Different Steganographic Algorithms for Secured Data Hiding, IJCSNS International Journal of Computer Science and Network Security, pp 154-160, 2010.

[14] B. S. Park, A. J. Choudhury, T. Y. Kim, and H. J. Lee, "A study on Password Input method using authentication Pattern and Puzzle," 2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), pp. 698–701, 2011.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143