ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Enhancement of Data Security for Cloud Environment Using Cryptography and Steganography Technique

Deepika

Research Scholar, Dept. of CSE, S.S.C.E.T, Badhani, Pathankot, India

ABSTRACT: Cloud computing offers quantifiability, accessibility and completely different services as vital advantages. However, as this new technology increasing it additionally discovers new risks and vulnerabilities too. In spite of being that varied structures and cloud services are growing, the perception of cloud computing has not been visualize. In simplest terms cloud computing suggests that storing and accessing knowledge and programs over the web rather than exploitation your own drive. Cloud users store their knowledge on cloud storage and that they needn't to stress regarding area issues, buying new storage instrumentation or manage their knowledge, they solely ought to access their knowledge at anytime from anywhere as long as they need net access. However owing to several security issues it ceased the organizations to attach with cloud computing fully. one among the most disadvantages of cloud computing is its large security risks. during this study varied security aspects of security problems has been analysed and so proposes a framework to mitigate security problems at the amount authentication and storage level in cloud computing. Economical security mechanisms ought to be deployed by suggests that of coding, authentication, and authorization or by another methodology to make sure the privacy of consumer's knowledge on cloud storage.

KEYWORDS:Cloud Computing, , Security, Steganography, Encryption, Decryption.

I. INTRODUCTION

Cloud computing is a new and emerging technology which is based upon the recent advances in technologies such as hardware virtualization, Web services, distributed computing, utility computing and system automation. Cloud computing securely and dynamically allocate physical resources such as computational power, storage, and networks to the users through virtualization. Also, Web Services are being used to delivered cloud resources to end-users. Ascloud computing helps organizations to sharpen their growth and performance. Besides this, it also hosts many users to provide entry to shared assets with less effort. However protection problems or threats are still a stumbling block in the success route of cloud computing. Numbers of explanations are the subject. First motive is that users and lots of corporations retailer their information on cloud storage, so the foremost focal point is the data need to be secure, and the info aren't being misplaced and tampered at the same time visiting from one location to another over the community. So it is fundamental that secrecy, accessibility and honesty of information ought to be guaranteed. Furthermore, unapproved get to the place an aggressor tries to be the impersonator of the approved shopper [3].

II. RELATED WORK

A hybrid encryption demonstrates utilizing grouping ordering, characteristics and time based systems. Information order is mostly in light of qualities. A hybrid ring was utilized to build up the security between the rings. These safely ensured rings play out the re-encryption keeping in mind the end goal to shield themselves from un-approved get to, time based, information proprietor demand and client repudiation. The outcome examination demonstrates that the hybrid ring model improves the unwavering quality and the effectiveness of the information security applications [1]. This paper [3]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

proposed an upgraded LSB based Steganography technique for pictures giving better information security. It shows an installing calculation for stowing away figured messages in nonadjacent and unpredictable pixel territories in edges and smooth areas of pictures. The edges in the cover-picture are recognized utilizing enhanced edge recognition channel. The scrambled message bits are then installed at all huge byte of arbitrarily chose edge pixels and some particular LSBs of red, green, blue segments separately. The paper[4] 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.Thispaper [5] presentsa review based ontheencryption mechanisms which are used tosolve various problemsin the cloud storage. They choose different problem definitions of different research papers and show that what the outcomes are by using encryption algorithms.This paper[6] describes that movement of client data toproviderimplies thatmove thecontrol over the datatothe cloud provider. However, for new customerschoosingthe rightinsuranceservices is sometimes difficult. So in thisarticle,the author describessome of the attributesthat identifythe policies ofsecurity and privacyservices. In [7] One new approach is defined named Trusted Cloud Computing Infrastructure (TCCI) which is based on Infrastructure security. TCCI approach describes that different nodes are required to run on secure environment so to keep hackers away. Moreover, if node runs in a secure environment than even administrator is incapable of access the user data. To make the infrastructure secure TCCI approach is proposed which handles the nodes by third party known as Trusted Coordinator (TC).

III. PROPOSED ALGORITHM

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.

A. *DESCRIPTION OF THE PROPOSED ALGORITHM:*

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.

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.

STEP 1: Image as an input and apply canny edge detection algorithm to find edges

The Canny edge detection algorithm has the following five stages:

a.Smoothing: Blur the image to remove noise.

b. Searching for gradients: Find the edge quality in the picture by bringing the slope with substantial magnitude.

c.Non-maximum suppression: Mark neighborhood maxima as edges.

d. Double thresholding: find viable edges by using computing thresholding.

e. Edge linking: Final edges are discovered through discarding all edges that are not connected to strong edges.

STEP 2: Dataset and convert it into binary form.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

STEP 3: Store those edges and their positions in an array and randomly select one index ofthat 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.
STEP 4: 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.
STEP 5: 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.

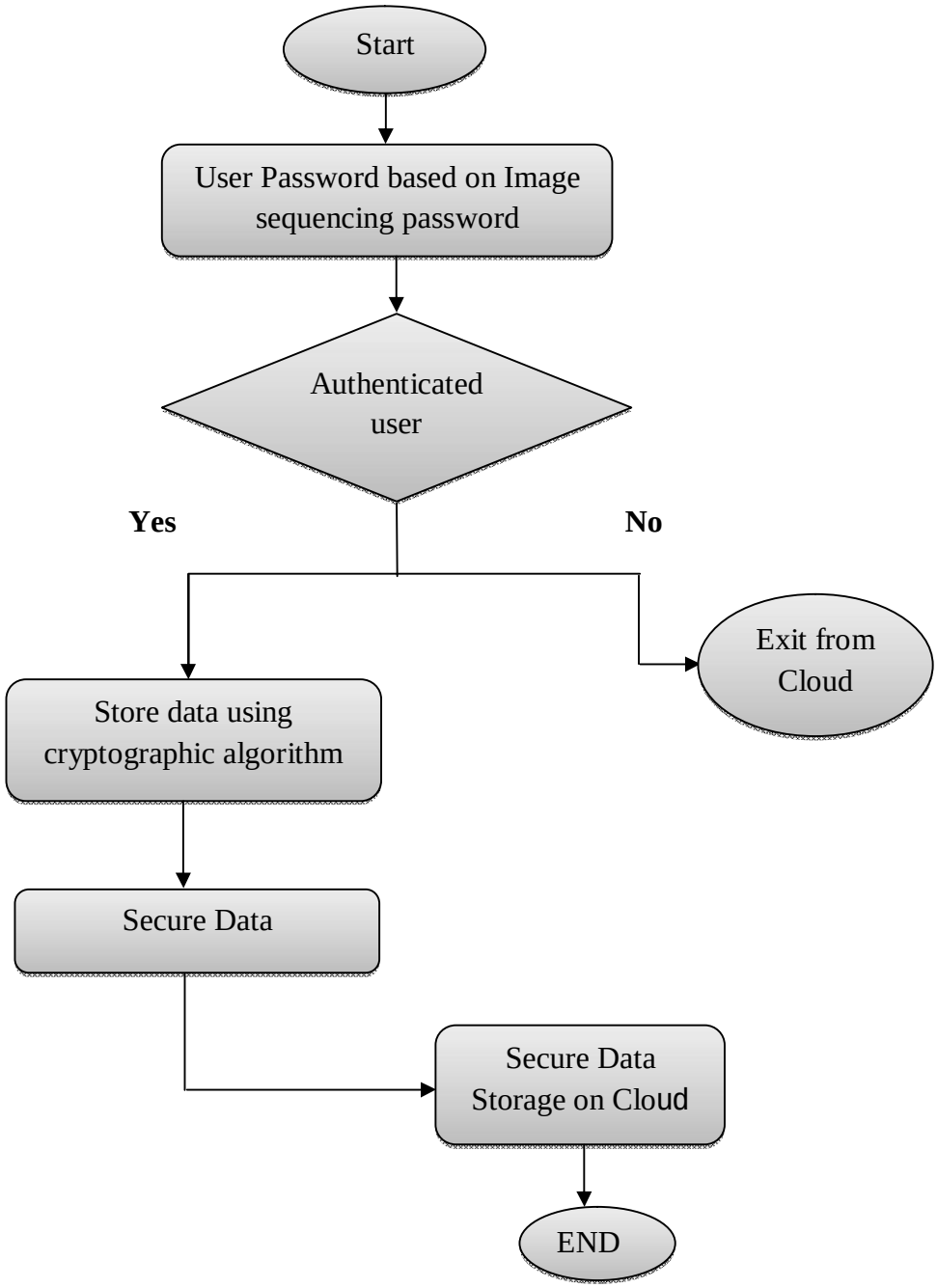

Fig 1: Flowchart of proposed methodology

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

IV. SIMULATION RESULTS

Simulation is the process of imitation of the operation of real-world process with respect to time. Simulation requires a model to be developed; this model should represent some key characteristics of a process. Simulation is used in many circumstances, for example simulation of technology for performance optimization, testing training, education and video games etc. to gain insight regarding functionality, scientific models of natural system are simulated. Simulation can be classified as live, virtual and constructive simulation. So, to represent the optimized result, we used cloudSim. CloudSim is a new generalized and capable of being stretched out simulation framework that capable of seamless modelling, simulation and experimentation of emerging cloud computing infrastructure and management services.CloudSim is a toolkit or a library used for simulation of cloud computing projects or allows researchers to the control every aspect of cloud environment such as algorithms, platforms, infrastructures. CloudSim helps to evaluate the performance of bottlenecks before deploying on real clouds by testing their services repeatedly and in controlled environment. CloudSim helps to compute the time for which services are accessed and compute amount a purchaser have to pay according to time and number of services consumed by the customer of cloud, who is using cloud resources at lease. The proposed methodology is implemented with the help ofCloudSimandNetBeansIDE8.0.CloudSimis the library that provides the simulation environment of cloud computing and also provide primary classes describing virtual machines, data centers, users and applications. Providing the library, Cloud Sim needs to develop a Java program using the components to create the desired structure or stage. However, Cloud Sim can be used to build a solution ready for use.On the other hand, Net Beansis a platform where applications are developed using segments called software modules.

The encryption and decryption data time has been illustrated in the following figure 1 and figure 2 with the comparison of existing system.

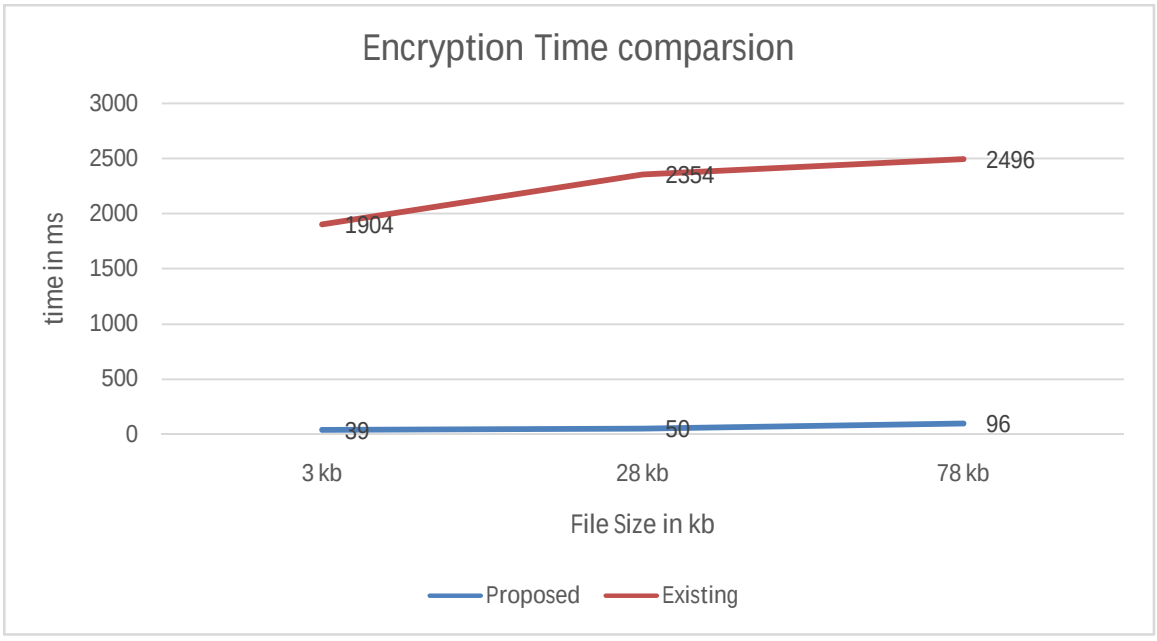

Fig 2.Tthe comparison of encryption time with the existing technique

The above figure shows the performance analysis of proposed system with the existing system. It is clearly analysed from the performance graphs that the proposed system is better than existing system. Figure 2 show the encryption time of with the existing system and improved system. The existing method takes encryption time 1904 milliseconds and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

proposed system takes time 39 milliseconds when the file size is 3 KB.When the file size is 78 Kb the existing method takes time in 2496 milliseconds and the proposed method takes time in 96 milliseconds.

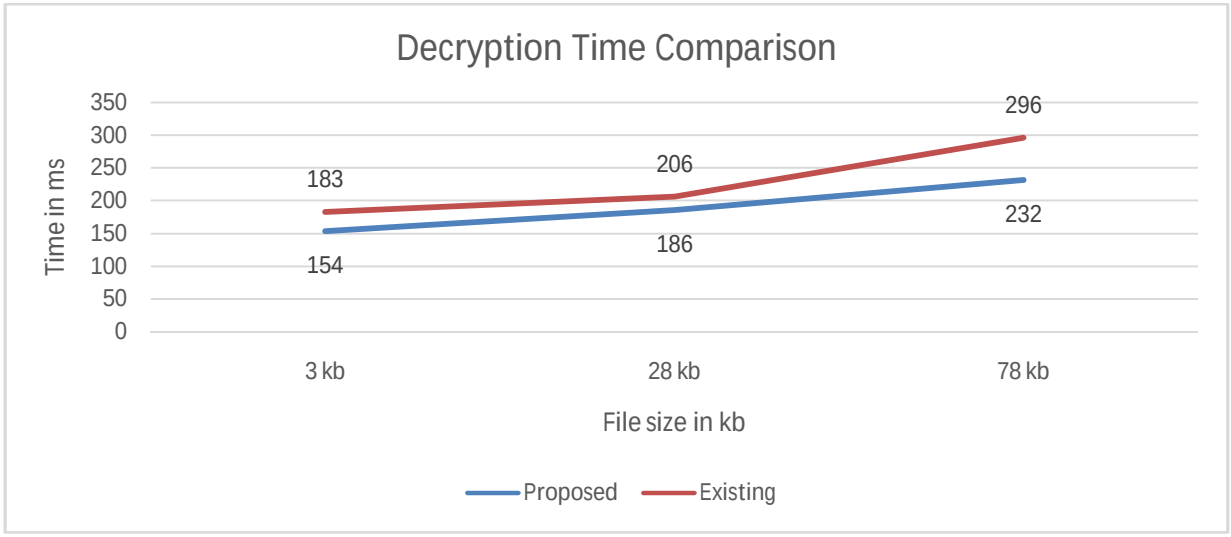

Fig 3 The comparison time of Decryption time with the existing technique

Figure 3. Shows the Decryption time between existing system and proposed system. The decryption time taken by existing system is 183 milliseconds and proposed system takes time in 154 milliseconds when file size is 3 KB.when we increase the file size up to 78 KB, the decryption time is taken by existing system is 296 milliseconds and proposed system takes only 153 milliseconds.

Therefore, in order to reduce the encryption and decryption time on cloud computing is according to security needs using machine learning algorithm. The above analysis shows the proposed methodology performs better in respect to data hiding time.

V. CONCLUSION AND FUTURE WORK

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. The experimental results show that the proposed technique performs better than the existing technique in terms of encryption time and decryption time. In future, some data classification approaches can be used to classify the data according to the security levels i.e. rather than encrypting the whole data in order to secure; first classify the data then encrypt only that data which need the more security that will more reduce the encryption time.

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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

[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] Abdullah, A., Hashim, F., & Al-Haddad, S. (2014) " A review of cloud security based on cryptographic mechanisms",*IEEE, Kuala Lumpur*, pp. 106-111.
[6] 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.
[7] 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
[8] 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
[9] 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.
[10] 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.
[11] 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.
[12] Pengfaidai and Chaokun Wang , "Software Watermark Approach Based Architecture for cloud Security", *14th Asia-Pacific Web Conference, APWeb 2012, Kunming, China*, pp. 270-281, 2012.
[13] Zhan Xin, Research on cloud computing data security Model based on multi-dimension, IEEE, 2012
[14] Zhao, G., Rong, C., &Jaatun, M. G. "Reference deployment models for eliminating user concerns on cloud security" Journal of supercomputing, Vol 61, Issue 2, pp 337-352, 2010.
[15] Usha, S., Kumar, G. A. S., and Boopathybagan, K., A secure triple level encryption method using cryptography and steganography, *Computer Science and Network Technology(ICCSNT), International Conference*, pp. 1017-1020,2011.
[16] MohemedAlmorsy Collaboration-Based Cloud Computing Security Management Framework, *IEEE International Conference on Cloud Computing (CLOUD)*,2011

BIOGRAPHY

Deepika is a Research scholar in the computer science Department, Sri Sai College of Engineering & Technology, Badhani, Pathankot. I received bachelor degree of Information Technology in 2013 from Sant Baba Bhag Singh College of Engineering and Technology, Khiala, Jalandhar, India. My research interests are Cloud computing security, cloudscheduling.