International Journal of Advanced Trends in Computer Applications

www.ijatca.com

An Approach to Enhance Multimedia Security in Cloud Computing

Harpreet Kaur[1], Er. Amandeep Kaur[2]
[1]Student (M.tech), Desh Bhagat University, Mandi Gobindgarh(India)
[2]Assistant Professor, Desh Bhagat University, Mandi Gobindgarh(India)

Abstract: *Nowadays multimedia has turn out to be essential in every domain for its quality. On the other hand, due to the problems of handling petabytes of such kind of multimedia data in words of calculations, sharing, communications, as well as stowage, there is a rising request of a substructure in the direction of having on-request admission towards a distributed group of configurable calculating assets. Cloud computing is the newest rebellion in IT industry which is fundamentally connected to the budget. The increasing amount of applications as well as the quantity of data which also essential to be accomplished has prepared information centers in the direction of turn out to be an significant as well as indispensable venture in addition to public cloud calculating give the impression to be a way in the direction of controlling these prices as well as their securities. The amalgamation of multimedia as well as cloud for security enhances many technical issues for numerous media-rich applications. In multimedia, there are various types of it such as audio, video, text, image etc. But in our work, we have utilized three kinds of multimedia data i.e. Text, Audio and Image data. In this paper, our main focus is on multimedia security in cloud computing. In our proposed work, we have utilized RSA, DES and Two Fish Algorithm to get inverted data. And also we have used genetic Algorithm for optimization purpose and to classify we have utilized neural network classifier. We have used parameter Mean Square Error and Signal-Noise-Ratio to evaluate our results as well as used these parameters to compare with existing work done by researchers. The over-all work is done and accomplished in MATLAB 7.10 environment.*
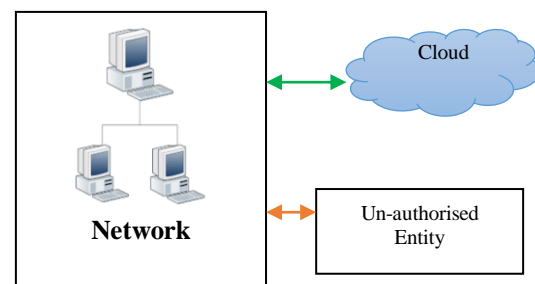
Keywords: *Cloud Computing, Multimedia, Internet, DES, AES, RSA, Security.*

I. INTRODUCTION

Rapid advances in broadband communication and high speed package switching network systems as well as the growing demand on multimedia file sharing have made effective multimedia data transmission and storage increasingly important. From the former few eras, there has a speedy progress in Cloud Computing. Cloud Computing provides an extensive variety of assets for instance computational platforms, stowage, computational power, and applications to operators by the use of internet. The foremost Cloud suppliers in the existing market sector are Microsoft, Google, Salesforce, Amazon, IBM and so forth.

Due to a growing amount of businesses/organizations rearranging in the direction of utilizing assets in the Cloud, there is 0inevitability for guarding the information of several clients. Some most important trials which are being confronted through Cloud Computing are to safe and sound, defend and handle the information that is the assets of the client. We have explained the two key states which also embrace

your information is available in the Cloud: the minute the information is in transit as well as after the data is at time out, wherever the information is much anticipated to be additionally safe. The further down exemplified are the two foremost circumstances that we have concentrated in the direction of understanding the need of security of the information and data in the Cloud.

Fig1: Unauthorized access of data between the network and Cloud

Above given figure explains about a situation in which a local network is associated towards a Cloud network, in

which some part of the network data is broken out from the local network and placed in the Cloud, nevertheless the perilous information be inherent in the specific local network itself. In this circumstance, the Cloud supplier does not have any kind of privilege of retrieving the information physically that is in the particular local network. But then again in several circumstances, the Cloud necessitates in the direction of accessing some data that is in the specific local network, throughout that access; there happens to be a probability of unsanctioned access of that specific local network assets.

It refer to the distinctive challenge in network safety wherever the data could aspect active in addition to passive assaults. The active assaults take account of amendment of messages, impersonating, replay assault, in addition to denial of service. Passive assaults comprises of traffic investigation. These assaults are to be expected to take place the minute the stream of data leaves the user network towards the Cloud network.

A. Essential Characteristics of Cloud Computing

As stated by NIST, the Cloud framework is made up of five important features [1]:

• **On-demand self-service:** A user could one-sidedly provision computing competencies, for instance server time interval in addition to network stowage, as required mechanically deprived of demanding human communication with every single service supplier.
• **Broad network access:** Competencies are obtainable through the network as well as handled by using customary mechanisms which also stimulate utilize by means of heterogeneous thin or else thick user stages (for instances, mobiles, laptops, tablets, as well as work places).
• **Resource pooling:** The supplier's computing assets are assembled to assist numerous users utilizing a multi-tenant framework, through dissimilar physical as well as simulated resources vigorously allocated as well as reallocated as stated by user request. There is an intellect of position individuality in which the user in general has no controller or familiarity over the particular position of the offered assets nevertheless this might be competent to stipulate position by the side of a greater level of abstraction (for examples, state, country, or information center). Instances of assets which also comprises of memory, stowage handling, as well as network bandwidth.
• **Rapid elasticity:** Competences could probably be elastically delivered as well as unconfined, in some circumstances mechanically, to measure promptly outward as well as inward proportionate through request. To the user, the proficiencies obtainable for provisioning frequently seem to be unrestricted as well as could be taken in any kind of magnitude at any time.

• Measured service: Cloud frameworks mechanically handle as well as augment resource utilize through leveraging a metering proficiency on round about some particular level of abstraction which is suitable to the category of service (for example, handling, storage, bandwidth, as well as vigorous client accounts). Asset usage could probably be scrutinized, handled, as well as testified, provided that pellucidity meant for both of the supplier and customer of the utilized service.

B. Requirement of Security in multimedia in cloud Computing

In cloud computing facility environments, there are several security problems similar to: cryptography traffic-handling, disseminated information processing, serviceability, virtualization, application security, access control as well as authentication, and so on. Specifically, Information access thru different assets which have need of access control system and consumer validation meant for joined control as well as managing in cloud computing surroundings [2]. Cloud computing security is a huge subject meant for research work, its freshness, thought-provoking and identification generated an application meant for researches in the direction of pursuing this subject in detailed. A lot of security anxieties progressed although evaluating the reimbursements of utilizing cloud computing above local assets. Further down are the foremost hazards which are presented by the cloud computing are:

Table 1: Security threats in multimedia

S. No.	Threats	Explanation
1.	Audit	Audit ability could be included as an extra layer over the virtualized operation framework facilitated on the virtual machine to give offices viewing what happened in the framework.
2.	Availability	The objective of accessibility for Cloud Computing frameworks is to guarantee its clients can utilize them whenever, at wherever [3].
3.	Confidentiality	This means preserving consumer's information secret inside the Cloud storage frameworks.
4.	Compliance	An automatic way to deal with checking and consistence will help get ready CSPs (Cloud Administration Supplier) and their clients to

		address rising necessities and the development of cloud plans of action [3].
5.	Control	Control in the Cloud system means to regulate the utilization of the framework, including the applications, its foundation in addition to the data.
6.	Data Integrity	Information trustworthiness in the Cloud framework intends to protect data integrity. As information is the base for giving Distributed computing administrations, for example, Information as an Administrations, Programming as an Administration, Stage as an Administration, keeping data integrity is a fundamental task
7.	Identity and Access Management (IAM)	The key critical success factor to managing individual identities at cloud providers is in the direction of having a vigorous amalgamated identity administration architecture in addition to approach internal towards the organization.
8.	Privacy	Security is an essential issue for distributed computing, both as far as legitimate consistence and client trust and this need to be considered at each period of configuration.
9.	Security-as-a [cloud] Service	Security-as-an administration is liable to see noteworthy future development for two reasons. Initially to shift in data security work from in-house to outsource will proceed. Second, data security needs to be available for associations.

II. PREVIOUS WORK DONE

Concerning this region of research and study, maximum research papers surveyed a standard old-style literature analysis process. A small number of papers gave a ground-breaking notion as well as anticipated a security prototypical.

F.A.Alvi et.al [3], inspected the security protection & trust issues of distributed computing. They have proposed a few overviews directed by IDC that demonstrate the inspiration for the appropriation of distributed computing. Additionally recognizes the issues and the answer for defeat these issues. It likewise contain the security model named security access control administrations SACS is dissected through the Hadoop guide diminish structure and the test results are gotten that contrast the framework execution and SACS model and without SACS model. When the assault begins up, the execution which utilizing security model is superior to not utilizing one. So the distributed computing with the proposed security model has the more stable performance when confronting the assault risk, particularly an assortment of stacks in the meantime.

Mandeep kaur et.al [4], surveyed the Encryption Algorithms to improve the Data Security in Cloud Computing. They have proposed to get to a cloud based web application that will attempt to dispose of the concerns with respect to information security; isolation. They additionally proposed diverse encryption calculations like - AES, DES, RSA and Blowfish to guarantee the security of information in cloud. They likewise expressed that the exploration will be directed utilizing Java runtime of Google App Engine, i.e. Eclipse IDE, JDK 1.6, Google App Engine SDK 1.6.0 or advanced. Sara Qaisar et.al [5], proposed Network/Security Threats and Counter Measures for distributed computing. This computation enhances associations execution by using least assets and administration support, with an imparted system, significant assets, transfer speed, programming's and equipment's in a practical way and restricted administration supplier dealings. Essentially it's another idea of giving virtualized assets to the shoppers. Purchasers can ask for a cloud for administrations, applications, arrangements and can store vast measure of information from diverse area. Be that as it may, because of continually increment in the prominence of distributed computing there is a continually developing danger of security turning into a primary and top issue. This paper is going to present the relative investigation of executing encryption calculation for securing the cloud.

Alzaber et.al [6], talks about that interactive media record stockpiling in distributed computing obliged the security. Sight and sound distributed computing is termed as media processing over frameworks, content conveyance system (it is utilized for diminish the dormancy and expand the transfer speed of information), server-based registering, and P2P sight and sound figuring. It gives foundation of elite figuring (HPC) viewpoint. J.Nieh et.al [7], recommended that Desktop figuring is Server-based sight and sound processing addresses in which all media registering is

done in a situated of servers, as well as the client cooperates just using servers. Wenwu Zhu et.al [8], depicted the diagram of sight and sound distributed computing and it gives tended to media distributed computing from sight and sound mindful cloud. Mixed media mindful cloud displayed how a cloud can give QoS bolster, circulated parallel handling, stockpiling, and burden adjusting for different sight and sound applications and administrations. It proposed a MEC-figuring structural engineering that can attain to high cloud QoS support for different sight and sound administrations. On cloud mindful sight and sound, we tended to how media administrations and applications, for example, stockpiling and imparting, writing and blend, adjustment and conveyance, and rendering and recovery, can ideally use distributed computing assets.

Jiann-Liang Chen [9] proposed a novel IP Multimedia Subsystem (IMS) system with distributed computing structural engineering for utilization in excellent media applications. The IMS bolsters heterogeneous systems administration with Quality-of-Service (QoS) approach. Tamleek Ali [10] proposed a structure for the utilization of distributed computing for secure scattering of ensured mixed media content and also records and rich media. They have utilized the UCON model for upholding fine-grained persistent utilization control imperatives on items dwelling in the cloud. Hang Yuan [11] gives an extensive diagram of the strategies and methodologies in the fields of vitality proficiency for server farms and vast scale interactive media administrations. The paper likewise highlights essential difficulties in planning and keeping up green server farms and recognizes a portion of the opportunities in offering green gushing administration in distributed computing systems.

Zhang Mian [12] introduced the study that depicts the distributed computing based interactive media database and the distinctive customary database, article situated database model of the idea, talks about the cloud-based item arranged sight and sound database of two ways, and condensed the qualities of such interactive media database model, prevalence and advancement. Chun-Ting Huang [13] conduct a profundity study on late media stockpiling security research exercises in relationship with distributed computing. Neha Jain [14] displayed an information security framework in distributed computing utilizing DES calculation. This Cipher Block Chaining framework is to be secure for customers and server. The security structural engineering of the framework is composed by utilizing DES figure square binding, which takes out the extortion that happens today with stolen information. Results to be secure the framework the correspondence between modules is scrambled utilizing symmetric key.
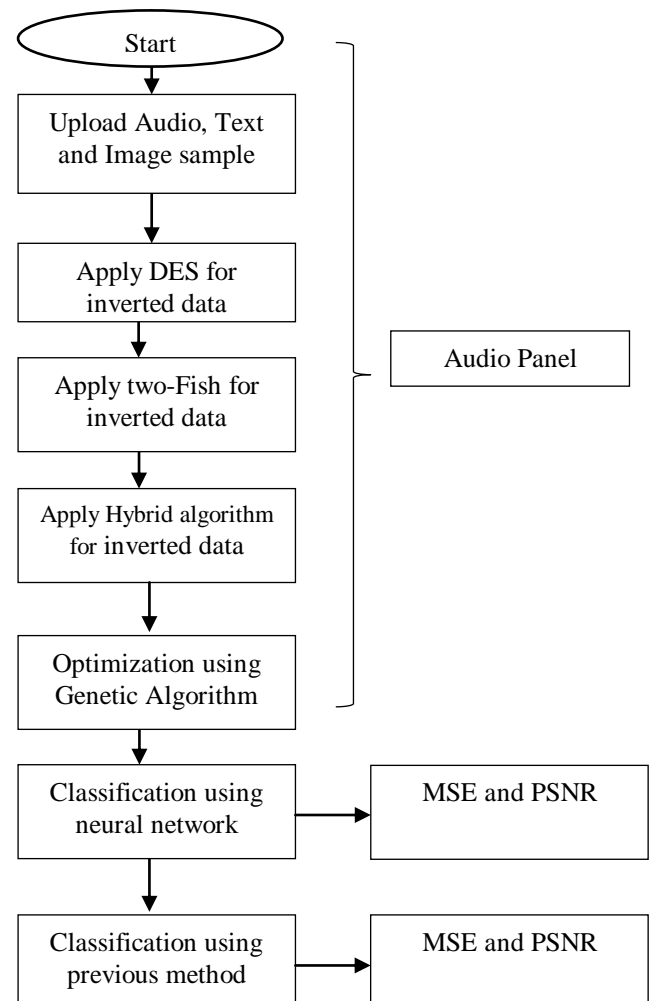
III. PROPOSED WORK MODEL

In our work we have worked using enhanced approach of security of the content which is going to be stored at cloud computing platform. In our proposed system, we have secured various kinds of multimedia data type using hybridization of DES, RSA and Two–wish algorithm. These algorithms are used together to make a much better and secured system as compare to existing system. In this we have used three panels separately for every multimedia type with their process are given below and its basic methodology is stated in steps given below:

Step 1 : Upload Data.

Step 2 : Once, text data is uploaded then we will apply DES for inverted data.
DES is a symmetric block cipher designed to encrypt and decrypt blocks of data consisting of 64 bits under control of sole 56 bit key. Every 8th bit of the particular 64-bit key is utilized on behalf of parity checking and if not then unnoticed. Decoding essentially be completed by utilizing the identical key as for encryption.

Fig 2: Flow Chart of BASIC Panel Work Model

Step 3 : After DES, apply Two fish Algorithm on previous output.

Two fish uses a 16-round Feistel-like structure along with further whitening of particular input as well as output. The solitary non-Feistel constituents are 1-bit rotates. The rotations could possibly be transported into the F operator in the direction of constructing a pure Feistel structure, however this necessitates a surplus rotation of the words just before the output whitening step. The plaintext is split into four 32-bit words. In the information enhancing step, these are cored with four keywords. This is followed by sixteen rounds. In each round, the two words on the left are utilized as information to the g capacities. The g capacity comprises of four all-inclusive key-subordinate S-boxes, trailed by a straight blending step taking into account an MDS matrix. The left and right halves are then swapped for the following round. After all the rounds, the swap of the last round is switched, and the four words are cored with four more key words to produce some cipher text.
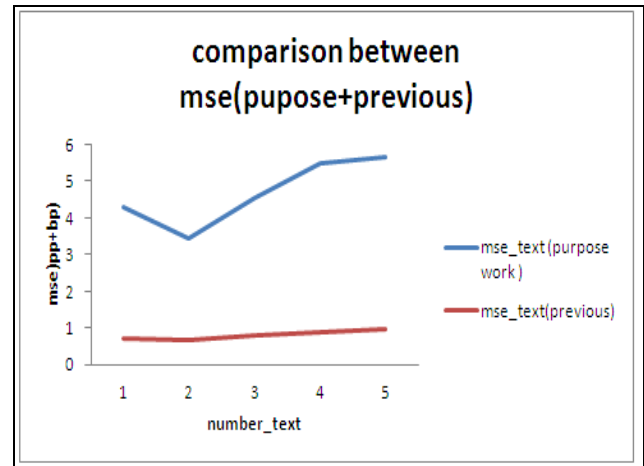
Step 4 : Then, apply Hybrid algorithm for inverted data.

Step 5 : After this we apply genetic algorithm for optimization purpose on the output attained from above.

Step 6 : Then later classify using neural network and get value of parameters MSE and PSNR.

Neural networks are those networks that are the collection of simple elements which function parallel. A neural network can be trained to perform a particular function by adjusting the values of the weights between elements. Network function is determined by the connections between elements. There are several activation functions that are used to produce relevant output.
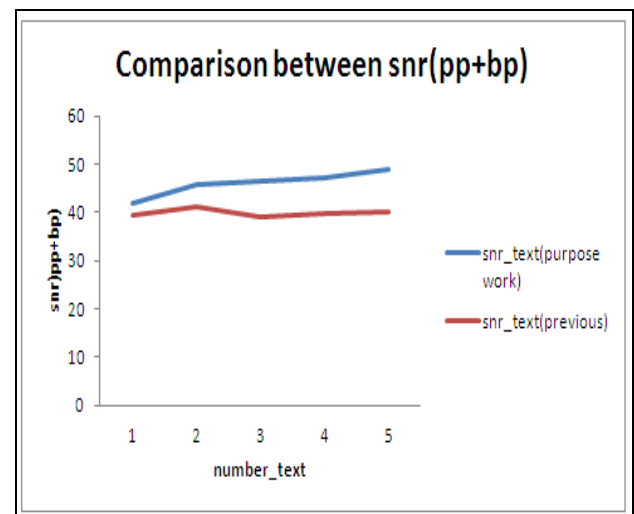
Step 7 : Then again classify using Previous Technique and get value of parameters MSE and PSNR. So, that it can be compared.

Similarly this process is followed in audio panel and image panel as shown by their flow chart below.
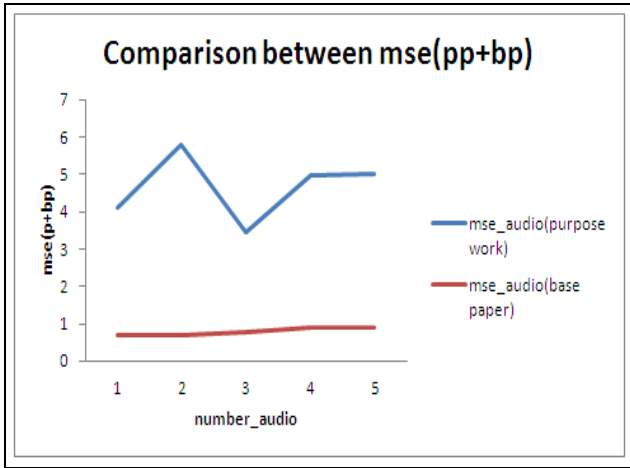
IV. RESULTS

Fig 3: Comparison between mse_text(purpose work + previous paper

In above comparison, we have compared the mean square error results of proposed work in text with the previous work done in text. Here, we have used blue colour for purposed work and red colour previous work. From above graph, we could state that mean square error result values of proposed work are better as compared to previous work done in text.
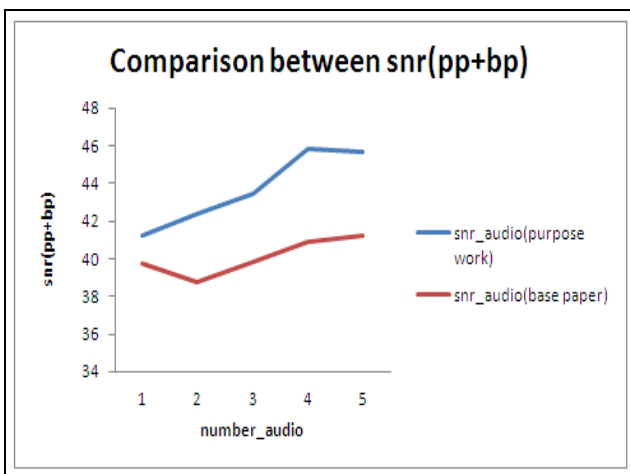

Figure 4: Comparison between snr_text(pp+bp)

In above comparison, we have compared the Signal noise ratio results of proposed work in text with the base paper work done in text. Here, we have used blue colour for purposed work and red colour base paper work. From above graph, we could state that signal error ratio result value of proposed work are better as compared to base paper work done in text.
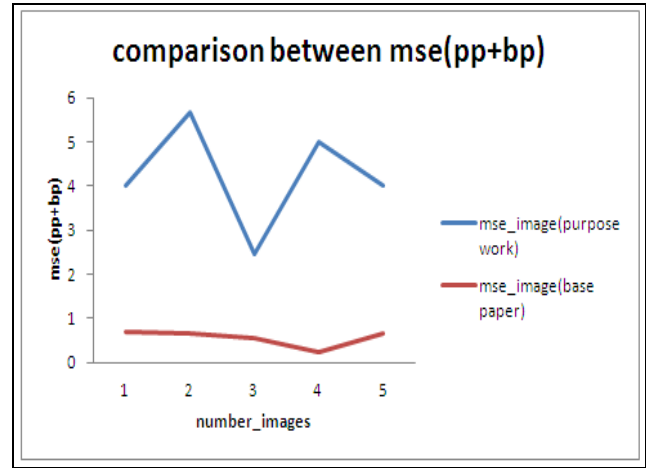
Figure 5: Comparison between mse_audio(pp+bp)

In above comparison, we have compared the Mean Square Error results of proposed work in audio with the base paper work done in audio. Here, we have used blue colour for purposed work and red colour basepaper work. From above graph, we could state that mean square error result values of proposed work are better as compared to base paper work done in audio.
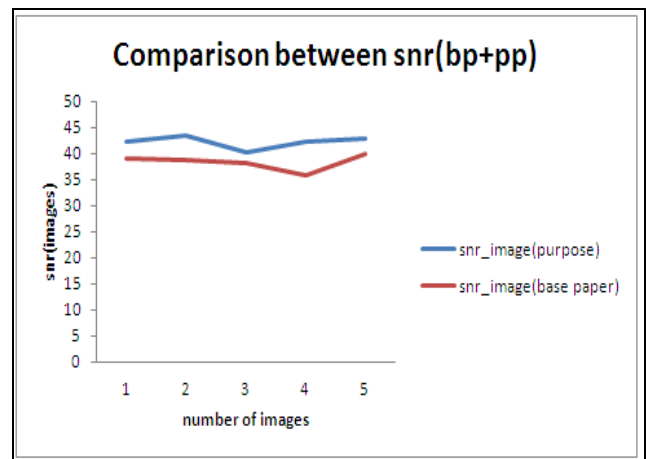

Figure 6: Comparison between snr_audio(pp+bp)

In above comparison, we have compared the Signal noise ratio results of proposed work in audio with the previous work done in audio. Here, we have used blue colour for purposed work and red colour previous work. From above graph, we could state that Signal noise ratio result value of proposed work are better as compared to previous work done in audio.
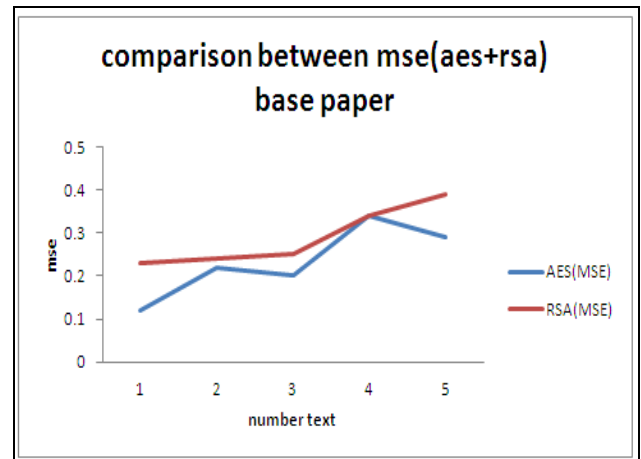

Figure 7: Comparison between mse_image(bp+pp)

Above graph shows the comparison between MSE values for image multimedia data between proposed and base algorithm. From graph it has been clear seen that MSE for proposed has value 6 and for base algorithm it is 1. So, proposed algorithm has good efficiency.

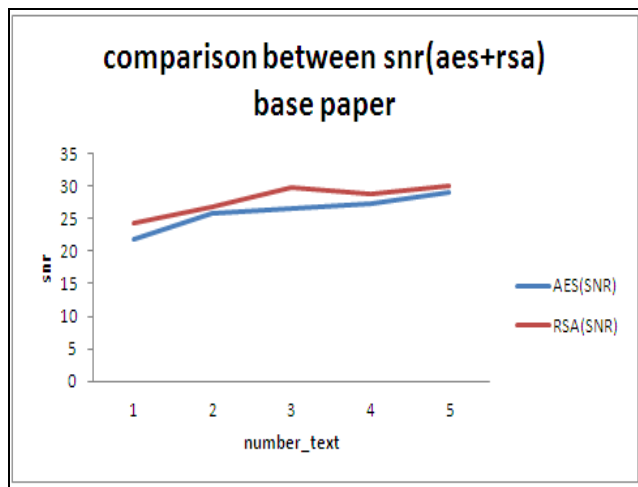

Figure 8: Comparison between snr_image(pp+bp)

Above graph shows the comparison between SNR values of proposed and base technique. From implementation it has been seen that SNR for proposed is 43 and for base is 39. SNR must be high to get good results.

Figure 9: Comparison between mse_text (rsa+aes (base paper))

Above graph shows the comparison between MSE values first by using AES algorithm and then by using RSA algorithm. From the graph it has been seen that MSE value for RSA algorithm is high w.r.t MSE value for AES.

Figure 10: Comparison between snr(aes+rsa) base paper

Above graph shows the comparison between SNR values first by using AES algorithm and then by using RSA algorithm. From the graph it has been seen that SNR value for RSA algorithm is high w.r.t SNR value for AES.

CONCLUSION & FUTURE SCOPE

This paper has presented the security model for multimedia cloud computing based on DES, 2-Fish, Genetic Algorithm and neural network based techniques. Earlier majority of work has been done in individual methods but this proposed work has implemented above mentioned techniques in hybridization with each other. From the results it has also been concluded that optimization parameter values for proposed algorithm is better w.r.t base algorithm e.g. obtained values of two parameters which are MSE is 4.3638 and SNR is 41.7322. In this we have also used various parameters of neural network e.g. Epoch 8 iterations, performance is evaluated as 37.8, gradient value is 0.963 and validation checks run on it are 6 for text multimedia data. For audio multimedia data obtained values of two parameters which are MSE is 16.6877 and SNR is 35.9068 and for Text data obtained values two parameters which are MSE is 5.9688 and SNR is 40.3719. In the end we have also done comparison of our proposed system with previous existing system and results shows that our proposed system is much better than previous one.

There are various types of multimedia data, in this paper audio, image and text data has been introduced but for future work video files can be introduced along with 3 files having same proposed methodology.

REFERENCES

[1] Peter Mell. (2011) 'The NIST Definition of Cloud ', Reports on Computer Systems Technology, sept., p. 7.

[2] Leena Khanna " Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them" Volume 3, Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[3] F.A.Alvi, B.S.Choudary, N.Jaferry,"Review on cloud computing security issues & challenges", iaesjournal.com, vol (2) (2012)

[4] Mandeep Kaur, Manish Mahajan, "Using encryption algorithms to enhance the data security in cloud computing, "International journal of communication and computer technologies", ISSN Number: 2278-9723.

[5] Sara Qaisar and Kausar Fiaz Khawaja," Cloud Computing:Network/Security Threats And Countermeasures", Ijcrb, January 2012 Vol 3, No 9.

[6] B. Aljaber, T. Jacobs, K. Nadiminti, and R. Buyya, "Multimedia on global grids: A case study in distributed raytracing," Malays. J. Comput. Sci., vol. 20, no. 1, pp. 1–11, June 2007.

[7] J. Nieh and S. J. Yang, "Measuring the multimedia performance of server based computing," in Proc. 10th Int.Workshop on Network and Operating System Support for Digital Audio and Video, 2000, pp. 55–64.

[8] Wenwu Zhu, Chong Luo, Jianfeng Wang, and Shipeng Li; "Multimedia Cloud Computing" Digital ObjectIdentifier 10.1109/MSP.2011.940269 Date of publication: 19 April 2011.

[9] Jiann-Liang Chen, Szu-Lin Wu, Yanuarius Teo filus Larosa, Pei-Jia Yang, and Yang-Fang Li; "IMS Cloud Computing Architecture for HighQuality Multimedia Applications" 978-1-4577-9538-2/11/$26.00 ©2011 IEEE.

[10] Tamleek Ali, Mohammad Nauman, Fazl-e-Hadi, "On Usage Control of Multimedia Content in and through Cloud Computing Paradigm, 978-1- 4244-6949-9/10/$26.00 ©2010 IEEE.

[11] Hang Yuan, C.-C. Jay Kuo and Ishfaq Ahmad; "Energy Efficiency in Data Centers and Cloud-Based Multimedia Services: An Overview and Future Directions" 978-1-4244-7614-5/10/$26.00 ©2010 IEEE.

[12] Zhang Mian, Zhang Nong; "The Study of Multimedia Data Model Technology Based on Cloud Computing"; 2010 2nd International Conference on Signal Processing Systems (ICSPS).

[13] Chun-Ting Huang, Zhongyuan Qin, C.-C. Jay Kuo; "Multimedia Storage Security in cloud computing : An overview"978-1-4577-1434-4/11/$26.00@2011 IEEE.

[14] Neha Jain and Gurpreet Kaur; "Implementing DES Algorithm in Cloud for Data Security" VSRD-IJCSIT, Vol. 2(4), 2012, 316-321.