International Journal of Advanced Trends in Computer Applications
www.ijatca.com

System Architecture for Secured Storage, Distribution and Delivery of Rich Multimedia information over the Content Delivery Networks and Cloud

Aafaq Ahmad Peerzada[1], Varinderjit Kaur[2]

[1]Aafaq Ahmad Peerzada
M.Tech CSE, Department of Computer Science and Engineering
Ramgarhia Institute of Engineering and Technology,Phagwara,Punjab
Peerzada.afaq@email.com

[2] Varinderjit Kaur
Associate Professor and Head, Department of Computer Science and Engineering and Technology
Ramgarhia Institute of Engineering and Technology, Phagwara, Punjab
vari_rupi@yahoo.co.in

Abstract: *Innovations in computing and with the increased popularity and usage of multimedia content, has added the new dimension to the ways of distribution storage and delivery of multimedia content across the internet. So the demand for secured data storage and transmission techniques across the internet has increased. Now since the cloud computing is practically possible and stake holders are looking the best possible ways to secure access to the shared resource pool and for that every loop hole is being looked in by the researcher's and possible solutions suggested. In this paper we have also tried to suggest a solution and created architecture for possible secured storage and distribution of multimedia content across the different content delivery networks .The architecture suggested has not only efficient hybrid encryption system but also focused on the ways of accessing the content and controlled utilization of bandwidth available to the end user. The hybrid of Blowfish and RSA algorithms applied and then optimized and classified the encrypted data, then stored on the available database, windows azure database used here. The proposed work finds its application in medical imaging systems, military image database communication and confidential video conferencing, and similar such application. The results of performance parameters are obtained through the use of MATLAB 7.10.0.The real time architecture developed and implemented in Microsoft .net platform with azure database as backend.*

Keywords: *RSA, Blowfish, Authentication, Multimedia, Cloud computing, Buffer Management. CDNs*

1. Introduction

Cloud computing as an innovation has redefined the boundaries of business computing and changed the IT industry from conventional software license business to service driven model, utilizing the already expanding virtualization technologies. This Integration of platform, software storage system and communication medium into a common shared resource pool has become a system of advanced computational power with high end storage capabilities. The main focus of cloud computing from the provider's view as extraneous hardware connected to support downtime on any device in the network, without a change in the users' perspective. Layering mechanism as proposed by Balding that should occur between the front-end software, middle-ware networking and back-end servers and storage, so that each part can be designed, implemented, tested and ran independent from subsequent layers. Though cloud computing is targeted to provide better utilization of resources using virtualization techniques and to take up much of the work load from the client, it is fraught with security risks. Cloud computing is an emerging technology with shared resources and lower cost that relies on pay per use according to the user demand.

The different cloud services are: Infrastructure as a service (IAAS), Software as a service (SAAS) and Platform as a service (PAAS) For any cloud computing data center IAAS, PAAS and SAAS paradigms are very important. It is assumed that in the Upcoming days the whole services is going to be provided by the cloud itself therefore the user

will need to pay for every Single type of service that the user uses [1].

2. Problem Statement

Multimedia data is a group of some of the following medium: content, audio, moving image, and film. By using multimedia information, the multimedia data can be transfer from users having transferable devices such as changeable phones. Multimedia data escape having issues of the material rights and the privacy and therefore defensive the multimedia in sequence becomes critical in multimedia used devices [1]. Since large amounts of multimedia information hold vast sizes, we require a competent encryption technique for defensive the multimedia data at the same time as satisfying the simultaneous necessity.

Due to the current development in computer network technology, giving out of digital multimedia passed through the internet is massive. Though, the augmented number of digital documents, compact disk processing tools, and the international ease of use of Internet access has created a very appropriate medium for exclusive rights fraud and disobedient distribution of multimedia content. A major condition now is to protect the scholar possessions of multimedia content in compact disk networks. There are figure of data types that can be characterize as multimedia data types. These are characteristically the basics for the building blocks of general multimedia environments, platform, or integrate tools. The essential type can be described as text, images, audio, video and Graphic objects. Multimedia finds its purpose in various areas counting, but not limited to, advertisements, art, education, entertainment, engineering, medicine, mathematics, business, scientific research and spatial temporal applications. Chiefly in Medicine, doctors can get qualified by looking at a virtual surgery or they can replicate how the human body is precious by diseases extend by viruses and microorganisms and then develop technique to prevent it [2]. So with the expansion of information message and computer technology, there has been the development of Digital hospital, Telemedicine in network by catalogue of digital medical image.

There are number of information sorts that can be described as interactive media information sorts. These are commonly the components for the building squares of mineral summed up mixed media situations, stages, or coordinating apparatuses [4]. The essential sorts can be depicted as takes after:

•**Text:** The structure in which the content can be put away can shift enormously. Notwithstanding ASCII based documents, content is commonly put away in processor records, spread sheets, databases and annotations on more broad media objects. With accessibility and expansion of GUIs, content textual styles the employment of putting away content is getting to be complex permitting enhancements (shading, shades...).

Images: There is awesome difference in the quality and size of capacity for still pictures. Digitalized pictures are succession of pixels that speaks to an area in the client's graphical showcase. The space overhead for still pictures changes on the premise of determination, size, many-sided quality, and pressure plan used to store picture. The prominent picture arrangements are jpg, png, bmp, and tiff.

Audio: An undeniably well-known information sort being coordinated in the greater part of uses is Audio. It's truly space concentrated. One moment of sound can take up to 2-3 Mbs of space. A few strategies are utilized to pack it in suitable arrangement.

Video: One on the most space devouring sight and sound information sort is digitalized feature. The digitalized features are put away as arrangement of casings. Contingent on its determination and size a solitary casing can expend upto 1 MB. Additionally to have practical feature playback, the transmission, pressure, and decompression of digitalized oblige consistent exchange rate [5].

2.1 SECURITY THREATS IN MULTIMEDIA

A. Inside assaults

There is plausibility for phishing and taking of media substance by the representative of the administration supplier itself.

B. Legal and theft troubles

There are more legitimate troubles on account of putting away media content in the web outside the limit i.e. Servers which are outside the nation. Likewise there are limitations in getting the media substance rights for diverse stages and imparting the media content outside the extent or utmost.

C. Migration

The client may think to move all his media substance to some other spot taking into account his adjustment in prerequisites. In any case, now the client does not have the opportunity of doing that [6].

Challenges over gauges

At present numerous merchants (individual who offers administrations) creating and propelling their own private cloud situations in light they could call their own conditions and security highlights which prompts issues in interoperability soon.

E. QOS

Clients going for questionable systems without their insight to offer the media substance despite the fact that there are accessibility of all the more encouraging gushing innovation and expanded broadband pace.

2.2 ADVANTAGES OF MULTIMEDIA DATA SECURITY

Media equipment offers number of key remuneration to its examine provider as well as the users from side to side enlarged completion time, well organized data storage capacity, less calculation and cost [7]. It shaped a striking crash in the multimedia content dispensation like editing, storing, encrypting and decrypting, gaming, stream, compress etc. Some more recompense is described below:

- **Cost**

Media compute offer cost effective military to its service provider through efficient multiplexing of media inside like audio, video, image by as long as a common infrastructure, utilize the server, optimization, virtualization, Mobility and habitual processing. There is no requiring for actually acquiring a communications or reserve in our local system and thus reduce the cost [8].

- **Upgradable**

Media is an always associated to the service supplier and consequently it is upgraded and maintain without any manual intervention. Software and security will be up to date constantly.

- **Compatibility**

Media allow the medium satisfied to be access anywhere through any smart mechanism and it is [9].

- **Storage**

Media knowledge has many bases for store the media content using the income. Also it is more sheltered since the store media contented will be duplicate without manual intrusion.

2.3 DISADVANTAGES OF MULTIMEDIA:

1. Expensive
2. Not always easy to configure
3. Requires Special Hardware
4. Not only Compatible [9].

3 . Related Work

A number of studies showing the need of security in the Multimedia file storage in cloud computing. Multimedia cloud computing is generally related to multimedia computing over grids, content delivery network (CDN) [42], server-based computing, and P2P multimedia computing. More specifically, multimedia computing over grids addresses infrastructure computing for multimedia from a high-performance computing (HPC) aspect [3]. The CDN addresses how to deliver multimedia at the edge so as to reduce the delivery latency or maximize the bandwidth for the clients to access the data. Examples include Akamai Technologies, Amazon CloudFront, and Limelight Networks. YouTube uses Akamai's CDN to deliver videos. Server-based multimedia computing addresses desktop computing, in which all multimedia computing is done in a set of servers, and the client interacts only with the servers [4]. Examples include Microsoft Remote Display Protocol and AT&T Virtual Network Computing. P2P multimedia computing refers to a distributed application architecture that partitions multimedia-computing tasks or workloads between peers. Examples include Skype, PPlive, and Coolstream.

Prof.Radha.S.Shirbhate, AnushreeA.Yerawar, Ankur M. Hingane[1], 2012, Security is necessary for the defines of delivery of multimedia data. Thus this security is providing by encryption. There are many encryption schemes are present for defensive multimedia data. In this paper, we are using discriminating encryption for defensive multimedia data. It takes less computational workload and provides five levels of security from level 0 to level 4.

K. Kalaivani and B. R. Sivakumar[2], 2012, this article, deal with the variety of techniques connected to security facet of Multimedia data, particularly the Medical data, their compensation and difficulty. The First Part describes the opening of Multimedia data and its use in Medical field. The Second part describes a variety of techniques that can be practical for General Multimedia data. The third Part describes a variety of techniques that can be applied to Medical images. The Fourth part describes requirement to get better the security of Medical data and the necessity of new algorithm for civilizing the security and quality of medical data capture by different image capture devices like ultrasonography , positron emission tomography, single photon emission computed tomography , optical imaging , computed tomography , X-ray, ultrasound, MRI etc.

Pravin Kawle, Avinash Hiwase, GautamBagde, kantTekam, Rahul Kalbande[11],2014,In today's globe most of the announcement is done using electronic media. Data Security is extensively used to make sure security in announcement, data storage and program. Security of compact disk data is a very important issue since of fast evolution of digital data uses the variation step, taking from Data Encryption Standard algorithm. An imaginary analysis and investigational have a fight prove that this method provide high speed as well as fewer connections or transport over unsecured network.

Multimedia data security is achieved by methods of cryptography, which deals with encryption of data. Standard symmetric encryption algorithms offer better safety for the multimedia data.

Raymond B. Wolfgang and Edward J. Delp[12], 1998, the increase of networked multimedia systems has created a need for the exclusive rights protection of digital images and video. Official document protection involves the verification of image content and/or ownership. This can be used to recognize illegal copies of an image. One move toward is to mark an image by adding an imperceptible structure known as a digital watermark to the image. Technique of incorporating such a watermark into digital images includes spatial domain techniques, convert domain algorithms and sub band filter approach.

LI Baoping 1, WANG Yan[13],2010,The instruction method of using multimedia equipment's in class improve schooling quality and competence, accelerating teaching reform in universities and colleges. However, sometimes it even harms the teaching effect. By doing surveys in four universities in Jiaozuo, and analyzing the advantages of using multimedia, this paper points out the problems in current teaching method and offers some suggestions and countermeasures. Thus multimedia technology could wield its magnificent power in education.

Adjeroh, Donald A., and Kingsley C. Nwosu [14], 1997, the spatial, temporal, storage, retrieval, integration, and appearance supplies of multimedia data differ significantly from those for customary data. A multimedia database organization system provides for the efficient storage and treatment of multimedia data in all its varied forms. We appear into the basic natural history of multimedia data, emphasize the need for multimedia DBMSs, and argue the supplies and issue required for increasing such systems.

Rajorshi Biswas[15], 2003,organization in both public and private sectors have become ever more dependent on electronic data processing. Defensive these important data is of utmost concern to the organization and cryptography is one of the primary ways to do the job. Public Key Cryptography is used to protect digital data going through an insecure channel from one place to another. RSA algorithm is expansively used in the popular implementations of Public Key Infrastructures. In this paper, we have done an efficient implementation of RSA algorithm using gimp library from GNU. We have also analysed the changes in the presentation of the algorithm by altering the number of typescript we are encoding together.

VANI.N, SREELATHA.P.K, PARVATHY.S [32], 2013, the blow of internet security is chief role in today's technology. To offer greater security for user data we propose VG-1 security algorithm. It provides well-organized and hopeful encryption and decryption algorithm. This algorithm uses encrypted private keys for generation of cipher text. The length of private key is more than 1024 bits. It recognizes all types of attacks performed by attacker such as Brute-force attack, sequence modification, timing modification, content alteration, and deception. VG-1 provide high security and tricky for attacker to decrypt and classify plain text. It provides greater routine, less delay and very well-organized encryption and decryption method when compare to RSA, DES, and AES and tripleDES.

Ajit Singh and Swati Mali [17], 2013, secure data is a difficult issue in today's era. Most of the information journey over the internet and it became complicated to make data secure. So Cryptography was introduced for making data secure. But alone cryptography cannot provide a better security move toward because the scrambled memorandum is still available to the eavesdropper. There arise needs of data hiding. So here we are using a mixture of steganography and cryptography for civilizing the security.

Rongxing et al [33] gave a new security and provenance proposal for data forensics and post examination in cloud computing. According to them their proposed system can provide the privacy and security on secret documents/files that are piled up in the cloud. It also provides secure authentication mechanism to control unauthorized user access, and provides track mechanism to resolves disputes of data. Their proposed secure provenance scheme is working on the bilinear pairing method .The strength of their work is the proposed secure provenance system and limitation of their work is that their proposed scheme is difficult to implement as it is based on complex mathematical model which is very difficult to understand.

La'Quata Sumter et al. [34] says: The rise in the scope of cloud computing has brought fear about the Internet Security and the threat of security in cloud computing is continuously increasing .To assure users that there information is secure, safe not accessible to unauthorized people, they have proposed the design of a system that will capture the movement and processing of the information kept on the cloud. They have identified there is need of security capture device on the cloud, which will definitely ensure users that their information is secure and safe from security threats and attacks. The proposed implementation is based on a case study and is implemented in a small cloud computing environment.

The advantage of their work is assurance of security to the end users of cloud. The limitation of this study is there proposed framework is not feasible for large scale cloud computing environments.

Mladen [35] states that Cloud computing is a recent field, which came into existence after years of research in networking and different types of computing. It uses a SOA, that minimized the information technology operating and maintenance cost for the clients, it offers greater flexibility, reduces capital costs, provides required services are along with many other characteristics. This study discusses issues associated with cloud computing along with Virtualization, Service oriented Architecture and end users. The study ranked security as the primary challenge in cloud computing. Service providers must assure the availability and reliability of services to the consumers available anytime, anywhere using internet, plus security, safety, data protection and Privacy is also exercised.
The benefit of this study is the identification of issues related with security and implementation. The drawback of this work is that study is based on theoretical concepts nothing practical found in this study.

Wenchao et al. [37] have explored the security properties of secure data sharing among the applications hosted on clouds. They have proposed a new security platform for cloud computing, which is named as Declarative Secure Distributed Systems (DS2). In DS2, the network protocol and security policies are specified Via Secure Network Data log (SeNDlog) a language which is normally rooted in Data log that merges declarative networking and logic-based access control specifications .They have added provenance support to the DS2 platform because they believe that the distributed Provenance is significant step towards a secure cloud data management infrastructure.
The strength of their work is the proposed tool for data centric security which provides secure query processing, seamless integration of declarative access control policies, system analysis and forensics, efficient end-to-end verification of data. Limitation is that there work has not been validated from cloud computing vendors.

Soren et al [38] have mentioned that benefits of clouds are shadowed with the security, safety and privacy challenges and due to these challenges the adoption of cloud computing has been inhibited to a great extent. In this paper an approach has been presented for analyzing security at client side and server side. Amazon‘s Elastic Compute Cloud (EC2) has been chosen for this assessment. The primary aim is to focus on the accessibility, vulnerabilities in the entire cloud infrastructure. They have implemented the security analysis model & weigh up it for realistic environments. Security assessment has been implemented in Python and weigh up was calculated on Amazon EC2.
The advantage of this work is their proposed tool which provides strong analysis of security attacks and vulnerabilities, this analysis helps vendors to improve their security policies and the drawback is that their proposed framework is specific to Amazon.

Flavi and Roberto [39] stated that clouds are being targeted increasingly day by day. In this paper integrity protection problem in the clouds, sketches a novel Architecture and Transparent Cloud Protection System (TCPS) for improved security of cloud services has been discussed. To address the integrity issues, they have proposed a system, and the system is named as Transparent Cloud Protection System (TCPS) for increased security of cloud resources. According to them their proposed system, TCPS can be used to keep the transparency and virtualization.
The strength of their work is their proposed tool which provides improved security, transparency and intrusion detection mechanism. The limitation of their work is that they haven‘t did not validate their work nor they have deployed in professional cloud computing scenario.

Wayne [40]: In this paper benefits of cloud computing are highlighted along with the basic security issues that are still associated with cloud services. Shaping the security of critical systems is very important. This research brings primary problems in terms of cloud security, which are alleged to cloud computing security and privacy issues. Key security issues identified and addressed in this paper are end user trust, Insider Access, Visibility, Risk Management, Client-Side Protection, Server-Side Protection, Access Control and Identity management.
The strengths of their work is identification and discussion on cloud computing security issues which educates end users about security and private risks associated with cloud services. The weakness is that they haven‘t proposed any tool or framework to address identified issues.

Jinpeng et al [41] said that Cloud computing poses many new security threats. In this paper they have evaluated these threats in depth from an image repository side. They have also analyzed the risks faced by the system administrators and end users of a cloud's image repository. An image management system design has been presented to address the associated risks and according to them the proposed design is implementable and proficient. The filters of the system in first step finds malicious stuff and in next step sensitive information like passwords etc are removed.
The strength of their work is the proposed image management system which provides image filters and

scanners to detect malicious images. The weakness is that image filters are not accurate and sometimes legitimate images may also be detected as malicious image and their virus scanner is also not efficient. The scanner is not capable to detect all types of viruses, virus scanner validation is not provided by the authors.

According to **Dan and Anna [42]** Cloud computing provides highly scalable resources accessed via Internet. Data protection problems in the cloud computing have not been tackled currently. In the cloud, users of cloud services have serious threat of losing confidential data. To address data privacy issues of users, they have proposed data protection framework. According to them the proposed data protection framework addresses the challenges throughout the cloud services life cycle.

4 . Proposed work and methodology

Cloud computing security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations. The processes will also likely include a business continuity and data backup plan in the case of a cloud security breach.
In this paper, we prospect the careful encryption advance for protecting multimedia data. Computational workload necessary for this encryption is very less [3]. Encryption on the whole means to change the message into code or twisted form, so that anybody who does not have the 'key' to decode the code cannot view it. This is frequently done by using a 'cipher'. A cipher is a type of algorithm used in encryption that uses certain describe method to mix up the data. The cipher can only be 'deciphered' with a 'key'. A key is the actual describe method' that was used to mess up the data, and hence the key can also decode the data When the data is unscramble by the use of a key, that is what is known as 'decryption'. It is the conflicting of encryption and the describe method' of scramble is essentially practical in invalidate, so as to decode it. Hence, the in a state and illegible text becomes decipherable once again. Devoid of encryption and explanation, there would be no 'security' in the network. So security is the main limitation while storing data over cloud server. Various security threats in cloud computing are Data loss, Leakage of data, User‘s authentication, Malicious users handling, Wrong usage of Cloud computing and its services, Hijacking of sessions while accessing data, insider threats, outsider malicious attacks, data loss, loss of control, and service disruption. Therefore enhancing the security for multimedia data storage in a cloud center is of paramount importance. Developing such an architecture which ensures the user that its data is secure is the main objective. To develop such a model, an adequate and insight knowledge of cloud computing has to be strong. Therefore the basic concepts and previous security measures taken in cloud computing must be studied and understood. The methods to store data in the cloud are studied. A three tier framework is developed to enhance security while storing multimedia files which includes identity based user authentication, encryption, and signature verification**.** The previous work discusses only about the safety majors but not about the encryption schemes.
The late development of arranged sight and sound frameworks has expanded the requirement for the security of computerized media. This is especially imperative for the security and implementation of protected innovation rights. Computerized media incorporates content, advanced sound, pictures, feature and programming.

Numerous methodologies are accessible for ensuring advanced information; these incorporate encryption, verification and time stamping. Anyhow, in this proposed work mixed media information can be secured utilizing hybridization of encryption calculations with machine learning calculations.

This would include a primary and normal user concept in which a primary user would get a normal download speed whereas the extended user would get high speed on buffering the data while download . The primary and the extended user would be decided based on subscription purchased. The signature in this scheme would also be a wave file bits. If the wave file bits of the uploaded signature would match with the bits of uploaded data at run time, only then the data would be downloaded. The proposed work will use various encryption algorithms like RSA and Blowfish.

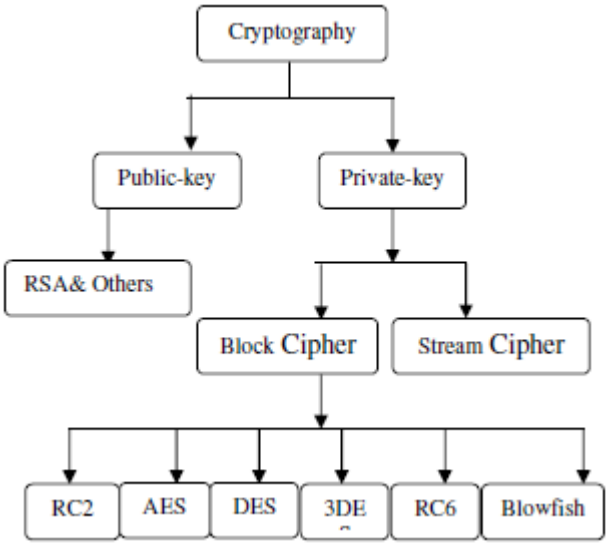

Figure1. Classification of Cryptographic techniques

5 . Design and Implementation

The study of performance parameters of Encryptions algorithms is tested and simulated on the Matlab. Encryptions followed by optimization , applying the genetic algorithm and using the neural network tool as classifiers giving the SNR and MSE values for all rounds of encrypted sample of outputted data. Hybrid encryption response time calculated based on the sample is done on the Matlab and experimental results calculated for the parameters like Signal to Noise ratio SNR for bandwidth utilization and we extended the real-time implementation to the Microsoft Azure cloud with code developed in .net and windows azure SQL server as backend database. Some additional security features added to framework are identify based authentication using login request generation and distribution of encrypted private key by the utilizing Gmail services. Stepwise details are as

Implementation Steps

1. User requests the login to authentication server and run
   Time key will received by the user on the registered email address and new user will have to register and acquire a subscription for download speed and Admin approves the subscription request after the payment verification.
2. User Uploads multimedia files i.e. audio file, text file,
   Image file and video file
3. Pseudo code is presented before user and a private key
   Send to the user on registered email.
4. Encryption Algorithms BLOWFISH followed by RSA on encryption are applied on uploaded data and data converted to slices or frames and stored on cloud database after the samples are optimized and then classified using the standard classifiers of cloud.
5. Uploading takes place on the basis of Signature and public /private keys.
6. Similarly admin can do steps from 2-4
7. For downloading matching of keys takes place along with digital signature and keys.
8. There are three subscription categories on the basis of which user can download data i.e. Premium, normal, high authority etc.
9. Users can download data after key and signature verification. The frames or data slices reassemble while downloading and the download of data will be controlled by the buffer management based on the Subscription category user belongs to. Live Streaming of downloaded files are also controlled by buffer management.

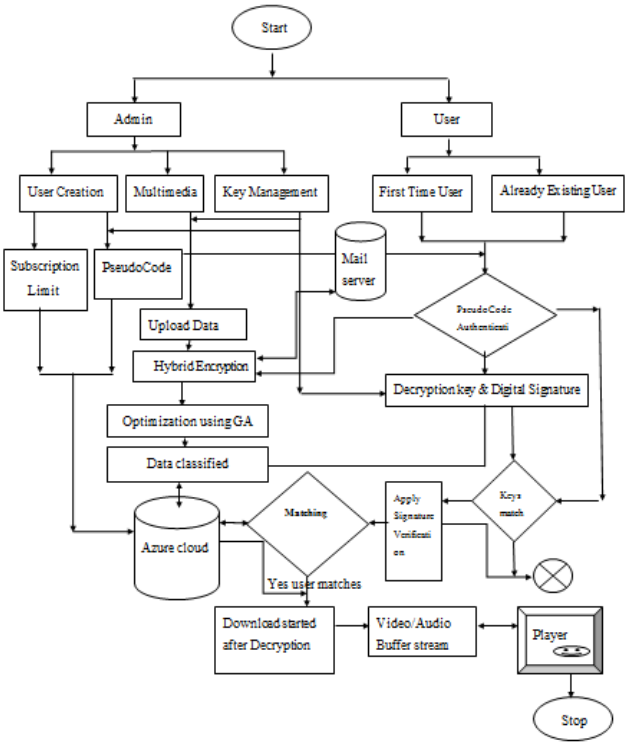

Figure-2 *System architecture for storing and retrieving Multimedia information*

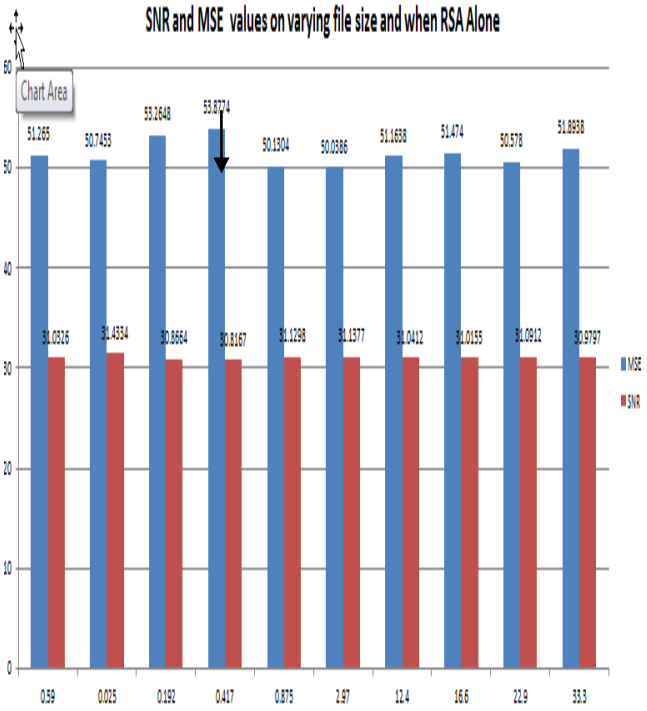

Figure -3(a) *SNR and MSE values for RSA*

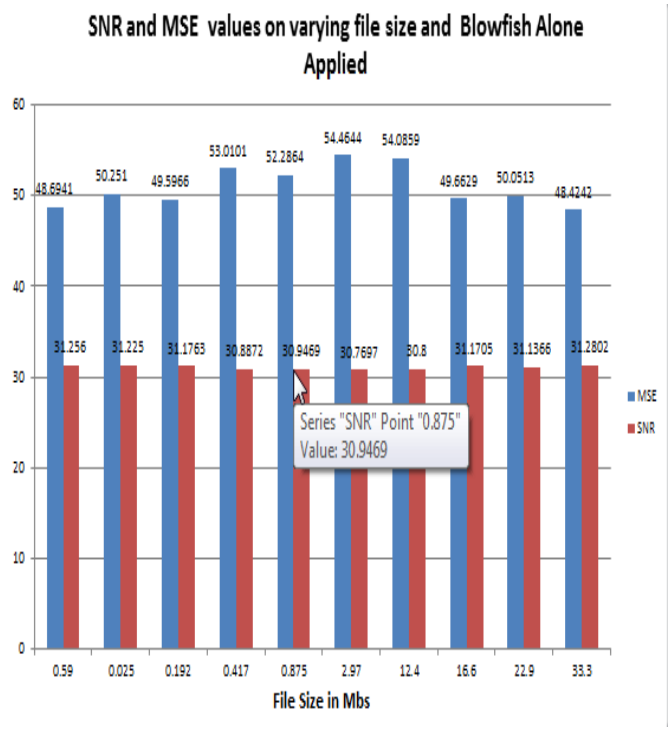

Figure -3 (b) *SNR and MSE Values for BlowFish alone*

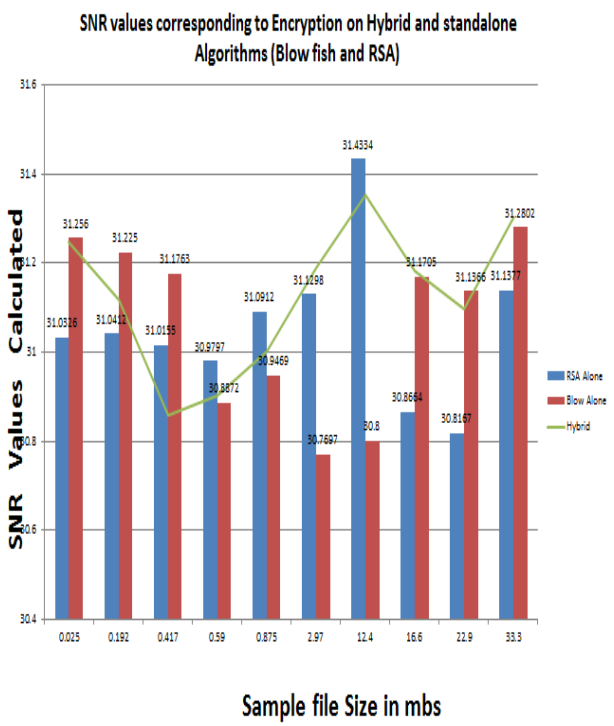

Figure -3 (d) *Relative SNR comparison*

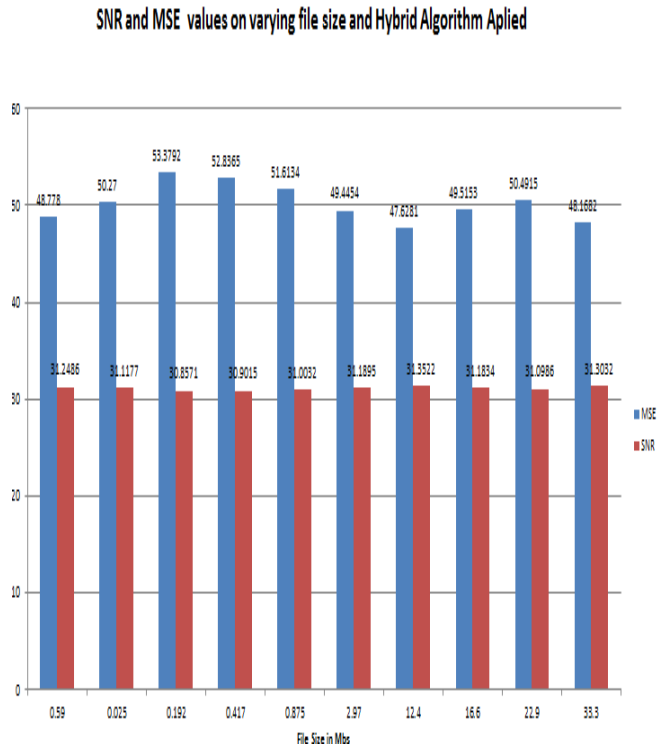

Figure-3(c) *Hybrid Approach Adopted*

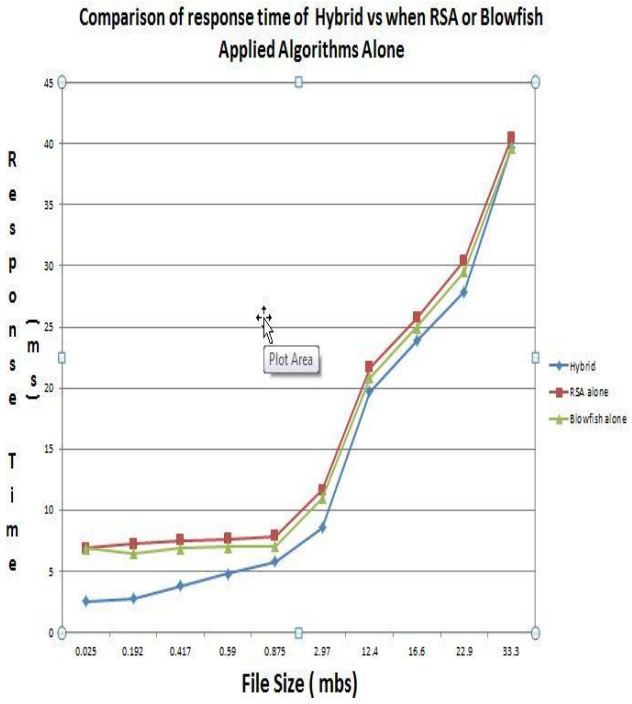

Figure -4 *Relative Response time comparison*

6. **Conclusion**

Because of the late advancements in PC organizing innovation, circulation of computerized interactive media content through the web is huge. Be that as it may, the expanded number of advanced records, interactive media preparing apparatuses, and the overall accessibility of Internet access has made an exceptionally suitable medium for copyright extortion and wild dispersion of sight and sound substance. A real

necessity now is to secure the licensed innovation of mixed media content in sight and sound systems. There are number of information sorts that can be portrayed as media information sorts. These are regularly the components for the building pieces of summed up interactive media situations, stages, or incorporating devices. The essential sorts can be depicted as content, pictures, sound, feature and Graphic articles. Interactive media thinks that its application in different territories including, however not restricted to, notices, workmanship, training, diversion, building, prescription, math, business, logical exploration and Spatial transient applications.

In this thesis hybridization of encryption calculations has been finished with hereditary calculation and additionally machine learning calculation to upgrade the security of the interactive media information. The two mixed media content that has been utilized is content record and discourse document. In this paper we have tried to realize the security schemes based on the efficiency of securing the interactive media disbursed across different storage platform in particular to cloud, So the prima concern is the ultimate secured distribution of all rich media content across the whole cloud and other high end access delivery points more efficiently with less latency issues than traditional P2P system but still under controlled access. We have tried to modify the versions of Blowfish and RSA created hybrid scheme, that has more efficiency in handling the sample data bits and reduce random error rate and lessen the execution time. We have shown that the proposed cryptosystem gives better encryption results in terms of security against statistical attacks. Even though it gives good security against statistical analysis it takes more time. So we propose that to reduce the time complexity one should reduce the number of rounds in Hybrid algorithm. So now area of improvement could be that the scheme could be applied to handling more no of data bits and more efficiency on bandwidth utilization on the delivery points and thus reducing the latency issue. Also model can replicated for the clouds environments build for B2C business model though private cloud type data centers have already adopted these check points along with already famous security apparatus.

References

1. Prof.Radha.S.Shirbhate,2Anushree A.Yerawar, 3Ankur M. Hingane," Features Preserving Data Encryption Used to Secure Multimedia Data", International Journal of Emerging Technology and Advanced Engineering Volume 2, Issue .1, January 2012.
2. K. Kalaivani and B. R. Sivakumar "Survey on Multimedia Data Security", JMO 2012 Vol.2(1): 36/41ISSN:2010-3697,DOI:10.7763/IJMO.2011. V1.82
3. A.Francia III, M. Yang, and M. Trifas "Applied Image.Processing to Multimedia Information Security," IEEE, 2009.
4. B. Furht, D. Socek, and A. M. Eskicioglu, "Fundamentals ofMultimedia Encryption Techniques," CRC Press, 2004.
5. C.-P. Wu and C.-C. J. Kuo, "Fast Encryption Methods for AudiovisualData Confidentiality," SPIE International Symposia on InformationTechnologies 2000, Boston, MA, pp. 284-295, 2002.
6. A. Servetti and J. C. De Martin, "Perception Based Partial Encryptionof Compressed Speech," IEEE Transaction on Speech and AudioProcessing, vol. 1, no. 8, 2002.
7. N. J. Thorwirth, P. Horvatic, R. Weis and J. Zhao ," Security methods for MP3 music delivery," Conference Record of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers, vol. 2, pp 1831-1835,2000.
8. S. Lian, D. Kanellopoulos, and G. Ruffo, "Recent Advances in Multimedia Information b System Security," Informatica, Vol. 33,pp. 3-24, 2009.
9. N. Kulkarni, B. Raman, and I. Gupta, "Multimedia Encryption: A Brief Overview," SCI 231, pp. 417-449, 2009.
10. Kalaivani, K., and B. Sivakumar. "Survey on multimedia data security."International Journal of Modeling and Optimization 2.1 (2012): 36-41.
11. Kawle, Pravin, et al. "Modified Advanced Encryption Standard.", International Journal of Soft Computing and Engineering, Volume-4, Issue-1, March 2014.
12. Wolfgang, Raymond B., and Edward J. Delp III. "Overview of image security techniques with applications in multimedia systems." Voice, Video, and Data Communications. International Society for Optics and Photonics, 1998.
13. LI, Baoping, and Yan WANG. "Analysis of the Advantages and Disadvantages of Multimedia Teaching in Colleges.",2010.
14. Adjeroh, Donald A., and Kingsley C. Nwosu. "Multimedia database management—requirements and issues." IEEE multimedia 4.3 (1997): 24-33.
15. Biswas, Rajorshi, ShibdasBandyopadhyay, and Anirban Banerjee. "A fast implementation of the RSA algorithm using the GNU MP library." IIIT–Calcutta, National workshop on cryptography. 2003.
16. Xu, Dingbang, and PengNing. "Privacy-preserving alert correlation: a concept hierarchy based approach." Computer Security Applications Conference, 21st Annual.2013.
17. Singh, Ajit, and Swati Malik. "Securing Data by Using Cryptography with Steganography." International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) ISSN 2277 (2013).
18. Shamily, P. Bindhu, and S. Durga. "A Review on Multimedia Cloud Computing, its Advantages and Challenges." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1.10 (2012): pp-130.

19. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. (2009, Feb. 10). Above the clouds: A Berkeley view of cloud computing. EECS Dept., Univ. California, Berkeley, No. UCB/EECS-2009-28 [Online]. Available:
20. R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," in Proc. 10th IEEE Int. Conf. High Performance Computing and Communications, 2008, pp. 5–13.
21. B. Aljaber, T. Jacobs, K. Nadiminti, and R. Buyya, "Multimedia on global grids: A case study in distributed ray tracing," Malays. J. Comput. Sci., vol. 20, no. 1, pp. 1–11, June 2007.
22. 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.
23. Wenwu Zhu, Chong Luo, Jianfeng Wang, and Shipeng Li; "Multimedia Cloud Computing" Digital Object Identifier 10.1109/MSP.2011.940269 Date of publication: 19 April 2011.
24. Jiann-Liang Chen, Szu-Lin Wu, Yanuarius Teofilus Larosa, Pei-Jia Yang, and Yang-Fang Li; "IMS Cloud Computing Architecture for High-Quality Multimedia Applications" 978-1-4577-9538-2/11/$26.00 ©2011 IEEE.
25. Li Li, Xiong Li, Sun Youxia, and Liu Wen; "Research On Mobile Multimedia Broadcasting Service Integration Based On Cloud Computing".
26. Tamleek Ali, Mohammad Nauman , Fazl-e-Hadi ,and Fahad bin Muhaya; "On Usage Control of Multimedia Content in and through Cloud Computing Paradigm".
27. 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.
28. Zhang Mian, Zhang Nong; "The Study of Multimedia Data Model Technology Based on Cloud Computing"; 2010 2nd International Conference on Signal Processing Systems (ICSPS).
29. Chun-Ting Huang, Zhongyuan Qin, C.-C. Jay Kuo; "Multimedia Storage Security in Cloud Computing: An Overview".
30. Neha Jain and Gurpreet Kaur; "Implementing DES Algorithm in Cloud for Data Security" VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321
31. Pravin Kawle,AvinashHiwase,GautamBagde, antTekam, Rahul Kalbande[3],2014, "Modified Advanced Encryption Standard"- International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-1, March 2014
32. Vani. N, Sreelatha P.K, Parvathy.S, Sridevi Malipatil," A NOVEL VSR ALGORITHM FOR NETWORK SECURITY OPTIMIZATION",Volume 2 :: Issue 2 :: IJRAET
33. Rongxing et al, ―Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing‖, ASIACCS,,10, Beijing, China.
34. R. La,,Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA
35. Mladen A. Vouch, "Cloud Computing Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246
36. Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande "Modified Advanced Encryption Standard "- ISSN: 2231-2307, Volume-4, Issue-1, March 2014 ,
37. Wenchao Zhou[Micah Sherr\ William R. Marczak] Z "Towards a Data-centric View of Cloud Security"
38. Soren Bleikertz et al, "Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds", CCSW 2010, Chicago, USA.
39. Flavio Lombardi, Roberto Di Pietro "Transparent Security for Cloud"
40. Wayne A. Jansen, _Cloud Hooks: Security and Privacy Issues in Cloud Computing_, 44th Hawaii,International Conference on System Sciesnces 2011.
41. Jinpeng et al, ―Managing Security of Virtual Machine Images in a Cloud Environment‖, CCSW, 2009, Chicago, USA
42. Dan Lin & Anna Squicciarini, ―Data Protection Models for Service Provisioning in the Cloud‖, SACMAT'10, 2010, Pittsburgh, Pennsylvania, USA
43. Xiaoming Bao, Rongshan Yu Institute for Infocomm Research, A*STAR, Singapore. "Streaming of Scalable Multimedia over Content Delivery Cloud"

Author's Profile:

Aafaq Ahmad Peerzada[1] is research Scholar of M.Tech CSE and has experience in SAAS Tenant integration testing, migrations and deployments .His interest area is researching technologies in area of cloud computing, Cryptography. SAAS Integration testing and tenant modular design in service delivery models, information and Network security, Data mining and Hadoop, Microsoft Technologies.

Varinderjit Kaur [2] **is** Heading the Department of Computer Science and Engineering, RIET Phagwara Jalandhar, Punjab India. She has got many research publications in National and International Journals in the field of Computer science. Her research interest areas are Cloud computing and information security, Data mining and wireless Networks.