The Study of Cloud Security and Data Centres Storage in Multi Media Cloud Computing

Navdeep Kaur[1], Er. Heena Wadhwa[2], Er. Harsimran Kaur[3]
[1]*Research Scholar, Department of IT, CEC Landran, Mohali, Punjab*
[2,3]*Assistant Professor, Department of CSE, CEC Landran, Mohali, Punjab*

Abstract **-** Cloud computing is a developing smartness of IT transferring that intends to make the Internet the ultimate home of all computing properties-storing, additions and accessibility. The next generation architecture of IT Enterprise is envisaged in Cloud Computing because of its strength, scalability, performance, high availability, least cost and many others. The transfer of Facilities by cloud Service Providers is hampered because of the security concerns shown by the Enterprises and dealers as the cloud situation gives access to centralized shared hardware, software and other information. The security matters in cloud computing such as service accessibility, massive traffic handling, application security, and authentication. Multimedia cloud computing has the probable for incredible benefits, but wide scale adoption has a range of challenges like Multimedia and facility heterogeneity, QoS heterogeneity, Network heterogeneity, Device heterogeneity ,Security, Power Ingestion that must be happened. But data security and access control is the main challenge when users outsource sensitive data for allocation on cloud attendants which is not within the same trusted domain as data owners. To keep sensitive user data private against untrusted servers, numerous methods have been proposed in the literature. The focus of this paper would be to cover protected storage and access methods of multimedia content over the content delivery cloud edge servers. This paper studies a new method which is a combination of roll based access control with advanced encryption algorithm (a combination of ARIA and ELGAMAL),signature verification to enhance security when storing text, image ,audio ,video files onto cloud server.

Keywords **-** Cloud computing, Security issues, secured storage, power computation and encryption techniques.

I. INTRODUCTION

In cloud-based multimedia-computing paradigm, users store and process their multimedia application data in the cloud in a dispersed manner, removing full installation of the media application software on the users‟ computer or device and thus assuaging the burden of memory requirement, multimedia software maintenance and upgrade as well as economical the calculation of user devices and saving the battery of mobile phones. Cloud computing multimedia [9] database is established on the present of database growth, object-oriented technology and object-oriented fields in the record, which growing display its vitality .Cloud computing provides a computer user access to Info Technology (IT) services which comprises submissions, servers, data storage, without requiring an understanding of the technology. A likeness to an energy computing network is to be valuable for cloud computing. To allowing convenient and on-demand network admission to a shared pool of configurable computing properties are used for as a prototypical of cloud computing. Cloud computing can be articulated as a grouping of Software-as-a-Service which refers to a service delivery model to enabling used for occupational services of system crossing point and can be joint creating new business facilities delivered via elastic networks and Display place as a Facility in which Cloud establishments donation an additional abstraction level which supplying a virtualized organization that can deliver the software platform where systems should be run on and Infrastructure as a Service which Suppliers accomplish a large set of computing resources which is used for loading and handling volume. Concluded Virtualization, they are talented to divided, allocate and animatedly re-size these resources to build ad-hoc systems as demanded by customers.

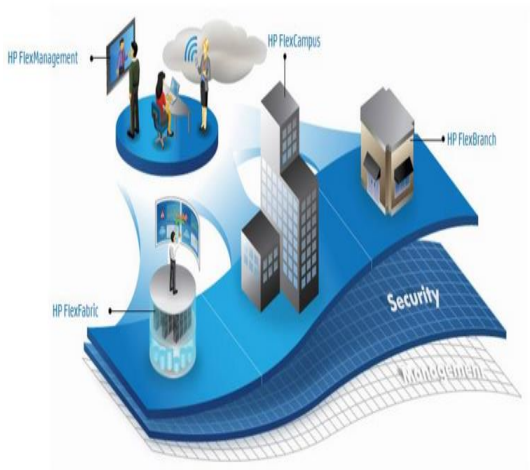

Fig.1: Management System

Internet multimedia is developing as a facility with the growth of Web 2.0. Hypermedia computing has appeared as a remarkable knowledge to generate, edit, process, and search media contents, such as imageries, video, audio, illustrations, and so on which deliver rich [4] media services. The management system is shown in figure no.1[4] For multimedia applications and conveniences in excess of the Internet and portable wireless schemes, at this time are

robust demands for cloud computing since of the important amount of calculation required for portion lots of Internet or movable operators at the similar time. In new cloud-based multimedia computing standard the operators stock and procedure their multimedia request information in the cloud in a disseminated manner, rejecting full connection of the broadcasting application system on the operators' computer or device and thus assuaging the burden of software maintenance and upgrade as well as sparing the calculation of user devices and saving the cordless of movable phones. Multimedia handing out in a cloud executes great challenges

Challenges in Multimedia Cloud Computing

Multimedia dispensation in a cloud executes great experiments. Numerous fundamental encounters for multimedia computing in the cloud are emphasized as follows.

1) Hypermedia and facility heterogeneity: As here exist dissimilar types of hypermedia and facilities, such as speech over IP (VoIP), video conferencing, photo sharing[10] and editing, multimedia flowing, image search, image-based translation, video beyond and edition, and hypermedia content distribution, the cloud shall provision dissimilar types of programme and multimedia facilities for lots of operators concurrently.

2) QoS heterogeneity: By way of dissimilar multimedia facilities have different QoS provisions, the cloud will deliver QoS provisioning and support for numerous types of multimedia services to meet unlike hypermedia QoS supplies.

3) Grid heterogeneity: By way of dissimilar systems, such as Internet, wireless local range grid (LAN), and third compeers wireless network, must different network features, such as bandwidth, interruption, and jitter, the cloud will adapt hypermedia contents for optimal delivery to numerous types of devices with different network bandwidths and latencies.

4) Security: As data is stored on the cloud and because of unreceptiveness nature of cloud, anybody can admittance the information on the cloud .Therefore security remains an important issue. As a consequence, security must be compulsory on data by using encryption plans to attain secured data storing and access.

5) Power Ingesting: The increasing scale and density of data centres [12] has made their power consumption an authoritative issue.. Moreover, a recent singularity has been the astounding increase in multimedia information transportation above the Internet, which in turn is applying a new weight on the energy resources.

Security Issues and Solutions

- A thoughtful safety subject arises in connotation with the expanding storage data centre of the cloud system, who supplies multimedia files of operators such as personal photos and videos.
- Top security concerns of cloud computing are Information damage, Leakage of information, Client's trust, User's authentication, Malicious users handling, Incorrect procedure of Cloud computing and its facilities, Hijacking of sessions while accessing data, insider[1] threats, outsider mischievous attacks, information loss, issues connected to multi-tenancy, damage of control, and service disruption.
- Therefore ornamental the safety for multimedia information storing in a cloud centre is of paramount importance.
- It is vital for the cloud storing to be armed with storage safety keys so that the whole cloud storage system is reliable and trustworthy.
- Several cloud storing security resolutions like bilinear pairing method, access mechanism, symmetric cryptographic algorithm like DES, RSA etc., unbalanced procedure like RSA have been developed rapidly in recent years, there must not yet understood a widely acknowledged model for the application.
- Besides the system design, the cloud storage security scheme must be flexible sufficient so that it can be better-quality by new cryptographic algorithms.

II. ADVANTAGES OF MULTIMEDIA DATA SECURITY

Media equipment offers number of key payment to its examine provider as well as the users from side to side distended completion period, well prearranged data storing volume, less calculation and cost[10]. It shaped a striking crash in the multimedia content dispensation like editing, stowing, encoding and decrypting, gaming, stream, compress etc. Some more recompense is described below:

A. Cost

Media compute offer cost effective military to its service earner through effectual multiplexing of broadcasting privileged like audio, video, image by as long as a shared substructure, exploit the server, optimization, virtualization, Flexibility and habitual processing. There is no necessitating for really obtaining a infrastructures or reserve in our local scheme and thus decrease the cost [9].

B. 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.

III. DISADVANTAGES OF MULTIMEDIA SECURITY

1. Expensive [8]
2. Not continuously relaxed to arrange
3. Needs Singular Hardware

IV. RELATED WORK

Prof. Radha.S.Shirbhate, Anushree A.Yerawar, Ankur M. Hingane[1],2012, Security is necessary for the defence of delivery of multimedia data. Thus this security was providing by encryption. There were many encryption schemes present for defensive multimedia data. In this

paper, they used discriminated encryption for defensive program data. It takes less computational assignment and delivered five levels of safety 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 described the opening of Multimedia data and its uses in Medical field. The Second part described a variety of techniques that can be practical for General Multimedia data. The third Part described a variety of techniques that can be applied to Medical images. The Fourth part described 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, solitary photon release calculated tomography , visual imaging , computed tomography , X-ray, ultrasound, MRI etc. Pravin Kawle, Avinash Hiwase [4],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 Normal procedure. An imaginary examination and untried have a fight prove that method provided high speed as well as fewer connections or transport over unsecured network. Multimedia data security was attained by approaches of cryptography, which contracts with encryption of data. Standard symmetric algorithms offer better safety for the multimedia data. Raymond B. Wolfgang and Edward J. Delp [5], 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[6],2010,** The instruction method of using multimedia equipments in class improve schooling quality and competence, accelerating teaching reform in universities and colleges. However, sometimes it even harms the education effect. By doing surveys in four academies in Jiaozuo, and analyzing the advantages of using multimedia, this broadside points out the difficulties in current teaching method and offers some suggestions and countermeasures. Thus multimedia knowledge could wield its magnificent power in instruction.

V. MULTIMEDIA SECURITY ENCRYPTION ALGORITHMS

A. ElGamal Algorithm

The security of ElGamal is based on the discrete logarithm problem. To encrypt and separately decrypt a message, a discrete power is executed. This procedure is efficient to compute. An enemy that seeks to decrypt an interrupted message may try to recover the private key. To this end a logarithm needs to be calculated. No actual method exists for this, given certain needs on the initial group are met. Under these conditions, the encryption is secure.

Now the ElGamal algorithm is used in many cryptographic products. The open-source software GnuPG uses ElGamal as standard for crosses. On behalf of this software and its difficulties with ElGamal discovered in late 2003 we will show the vital of correct implementation of cryptographic algorithms [3].

B. Encryption Algorithm

- This is a block cipher with the following characteristics [7]:
- ARIA quarters key sizes of 128, 192, and 256 bits, and the block size is 128-bit long.
- ARIA uses a 16 × 16 evolutional binary matrix with maximum branch number of 8 as its diffusion layer.
- ARIA uses the same algorithm for encryption and decryption, taking advantage of its evolutional diffusion matrix.
- ARIA is designed to resist many known attacks on block ciphers, counting difference cryptanalysis and lined cryptanalysis.
- ARIA is designed to be efficient both in software and hardware implementations.

C. Des Algorithm

It is a symmetric encoding scheme that uses 64-bit chunks, 8 bits (unique octet) of who are used for equivalence verify (to confirm the key's integrity). Each of the key's parity bits (1 every 8 bits) is used to verify one of the solution's octets by odd equivalence, that is, each of the parity bits is adjusted to have an odd amount of one's in the octet it fits to. The key therefore has a [10] "useful" length of 56 bits, which means that individual 56 bits remain really used in the procedure. The procedure involves carrying out combinations, substitutions and variations among the text to be encoded and the significant, while making sure the operations can be performed in both directions (for decode). The mixture of replacements and variations is called a product code.

VI. CONCLUSION

The Cloud computing as a expertise would be accepted if the extents of worries like safety of the data will be covered with full proof mechanism.A protected three tier construction in which novel file (text, audio, video, image) is stored on local server, the encoded file-name and the account of the novel file is stored on cloud server and to decrypt the file user has to arrive secluded key which is

stored in its Gmail profile. The strength of cloud computing is the aptitude to achieve dangers in specific to security matters. The model will present an outline sketch of architecture to be adopted by architects involved in implementing the cloud computing. Safety procedures stated for encoding and decoding (aria and elgimal) and ways proposed to access the multimedia content can be implemented in planned to enhance security framework over the network.

VII. REFERENCES

[1] Adjeroh, Donald A., and Kingsley C. Nwosu. "Multimedia database management—requirements and issues." IEEE multimedia 4.3 (1997): 24-33.

[2] Biswas, Rajorshi, Shibdas Bandyopadhyay, and Anirban Banerjee. "A fast implementation of the RSA algorithm using the GNU MP library." IIIT–Calcutta, National workshop on cryptography. 2003.

[3] Elgamal, Taher. "Method and apparatus for providing electronic accounts over a public network." U.S. Patent No. 6,138,107. 24 Oct. 2000.

[4] Kalaivani, K., and B. Sivakumar. "Survey on multimedia data security."International Journal of Modeling and Optimization 2.1 (2012): 36-41.

[5] Kawle, Pravin, et al. "Modified Advanced Encryption Standard.", International Journal of Soft Computing and Engineering, Volume-4, Issue-1, March 2014.

[6] LI, Baoping, and Yan WANG. "Analysis of the Advantages and Disadvantages of Multimedia Teaching in Colleges.",2010.

[7] Li, Shenhua, and Chunyan Song. "Improved impossible differential cryptanalysis of ARIA." Information Security and Assurance, 2008. ISA 2008. International Conference on. IEEE, 2008

[8] Menezes, Alfred J. Elliptic curve public key cryptosystems. Vol. 234. Springer Science & Business Media, 2012.

[9] 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.

[10] 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

[11] 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)

[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 Optics and Photonics, 1998.

[13] Xu, Dingbang, and Peng Ning. "Privacy preserving alert correlation: a concept hierarchy based approach." Computer Security Applications Conference, 21st Annual.2013.

.