SECURITY ENHANCEMENT WITH ENHANCED ARIA ENCRYPTION POLICIES FOR MULTIMEDIA STORAGE

[1] Navdeep Kaur, [2] Er.Heena Wadhwa

[1]Research scholar, [2]Assistant Professor,
[1] Department of IT, [2]Department of CSE
[1]CEC Landran, Mohali, Punjab

Abstract : ***Cloud Computing has become famous due to its effective characteristics. Various service that cloud server provide to their users to manage online processing, Storage drives and lots of other useful services. Storage of data elements is very critical process in this area. Due to various security attacks cloud servers manage their data in terms of encoded storage. Security against the attacks is main challenge in cloud storage. In this paper, A hybrid approach proposed to decrease the probability of decryption if the data accessed by attack during the transmission or storage in cloud computing. This is two phase authentication process that includes authorization and decryption for stored data elements on cloud server. As in previous theories of researcher lack of accuracy factor and time consumption issue, this research is provide secure and high accuracy rate along with fast processing speed for cloud storage. Overall process will provide less time for processing and less probability factor due to two phase authentication and encryption process with Aria and Elgamal hybrid policy.***

IndexTerms - Cloud Computing, Cloud Services, Hybrid approach, encryption process.

I. INTRODUCTION

Cloud computing services can be used from varied and prevalent property, slightly than distant servers or confined equipment. There is rejection normal description of cloud compute. Normally it consists of a group of dispersed servers recognized as masters, given that require services and possessions to dissimilar clients recognized as customers in a system with scalability and dependability of datacenter [1].

The dispersed computers offer on requirement services. Examination may be of software possessions (e.g. software as a service, SaaS) or corporeal possessions (e.g. platform as a service, PaaS) or hardware/communications (e.g. hardware as a service, HaaS or communications as a Service, IaaS). Amazon EC2 (Amazon stretchy Compute Cloud) is a case of Cloud Computing examination [2].

The cloud does appear resolve some ancient issues with the still growing costs of apply, preserve, and supporting an IT communications that is rarely utilized everywhere near its ability in the single-owner atmosphere. There is a chance to amplify competence and reduce expenses in the IT section of the commerce and decision-makers are commencement to pay concentration. Vendors who can supply a protected, high-availability, scalable communications to the loads may be poised to be successful in receiving association to accept their cloud services [3]. The cloud computing advantages are:

- Elasticity
- Adversity Improvement
- Mechanical Software –update
- Improved Association
- Environment Responsive
- Storage

The cloud computing disadvantages are:

- Technical Problems
- Security in the cloud
- Horizontal to Attack

There are a number of data types in use today that can be characterized as multimedia data types. These are the fundamentals used for the construction blocks of other comprehensive multimedia settings, platforms, or incorporating tools. The elementary types can be described as follows [4]:

-*Texture :* The form in which the text can be stored can vary greatly. In addition to the ASCII based files, text is typically stored in processor files, spreadsheets, databases and annotations, on more general multimedia objects. With availability and proliferation of GUIs and text fonts, the job of storing text is becoming complex allowing special effects.

-*Image:* The great quality and size of storage for still images. Digitalized images are categorization of pixels that signifies a region in the user's graphical display. The space above for still images varies on the basis of resolution, size, complexity, and compression scheme used to store image. \

-*Audio:* An progressively general data-type being united in most of requests is Audio. It is quite space intensive. One minute of sound can take up to 2-3 Mbs of space. Several techniques are used to compress it in a suitable format.

-*Video:* One on the maximum space-consuming multi-media datatype is digital video. The digitalized videos are stored as order of frames. Contingent upon its determination and size a single frame can consume up to 1 MB.

II. MULTI-MEDIA CLOUD COMPUTING

The growing popularity of the cloud computing platforms, multimedia mails, composed presentations, high-quality audio and video, collaborative multimedia documents and other rich media applications can be stored in the cloud data storage server[5].

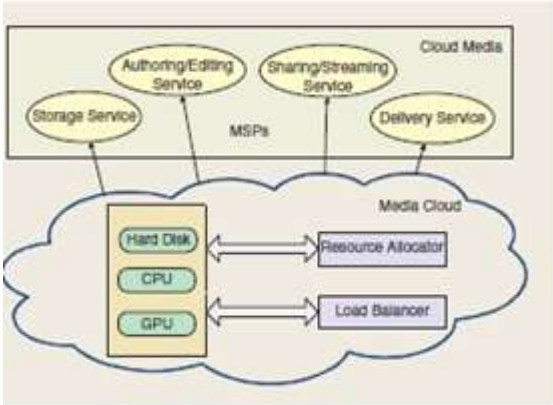

Fig 1. Relationship in media cloud and cloud services

This is utilized by an everyday increasing number of cloud users who can easily access the multimedia content over the internet at any time. The consumer can proficiently store the multi-media contented of any kind and of any size in the cloud after subscribing it with no difficulties. Not only the storing of the media content like Audio, Video and Image, but can process them within the cloud since the computation time for processing media data is more in complex hardware. After dispensation the treated data can be easily established from the cloud through a client without any necessity of installing complex hardware. Multimedia cloud computing is the processing, accessing and storing of multimedia contents like audio, video and image using the services and applications available in the cloud without physically acquiring them. Several fundamental challenges for multimedia computing in the cloud are highlighted as follows:

- Multimedia and service heterogeneity
- QoS heterogeneity [6]
- Network heterogeneity
- Device heterogeneity

III. Related Work

Marie-Francine Moens et al., 2016[7] defined that the multimodal information fusion both at the signal and the semantics levels is a core part in most multimedia applications, including multimedia indexing, retrieval, summarization and others. Early or late fusion of modality-specific processing results has been addressed in multimedia prototypes since their very early days, through various methodologies including rule-based approaches, information-theoretic models and machine learning. Visualization and Language are binary of the major modalities that are being attached and which have concerned special attention in worldwide tasks with a long history of results, such as TRECVid, ImageClef and others. During the last decade, vision-language semantic integration has attracted attention from traditionally noninterdisciplinary research communities, such as Computer Vision and Natural Language Processing. This is due to the fact that one modality can significantly assist the dispensation of another if prompts for disambiguation, complementary information and noise/error filtering. The latest boom of deep learning methods has opened up new directions in joint modelling of visual and co-occurring verbal information in multimedia discourse. **RAMESH.B et al., 2013 [8]** discussed the principal concepts of multimedia cloud computing to present a framework to address a multimedia cloud computing from multimedia-aware cloud (media cloud) and cloud-aware multimedia (cloud media) perspectives. Firstly, a media cloud, addresses its performance in distributed multimedia processing and storage to provide quality of service (QoS) provisioned for multimedia services. A media-edge cloud (MEC) architecture was proposed for high QoS for multimedia services, in central processing unit (CPU), and QoS adaptation for several devices. Later, a cloud media, addresses how multimedia services and applications, like: storage and sharing, authoring and mashup, adaptation and delivery, and rendering and retrieval, can optimally utilize cloud-computing resources to achieve better quality of experience (QoE). The deployment and distribution issues and outline future directions were discussed concentrating on audio-visual services of mobile multimedia applications for its delivery on mobile devices. **P.Bindhu Shamily et al.,2012[9]** presented that cloud computing was an internet service for data accessing, computation and storage with scalability, flexibility and low cost. It was a generation next platform for computation that offers several services to user without physically acquiring them. Public clouds are available for general users based on pay per use. On the other hand, in private cloud, user develops own application and runs their own infrastructure. The integration of both public and private cloud was the Hybrid cloud. The major goal of cloud computing is managing and processing the multimedia content. The Multimedia cloud computing and its services, is most challenging advantages of cloud media. **Alessio botta et al.,2016 [10]**presented that the cloud computing and Internet of Things (IoT) are two very different technologies that are already part of our life. Their implementation and use are probable to be more and more prevalent, making them significant components of the Future Internet. The integration of Cloud and IoT is known as CloudIoT paradigm, cause major change in several application scenarios. Cloud and IoT were surveyed separately and more precisely for their features, properties, underlying technologies, and open issues. The adoption and nanalysis of CloudIoT paradigm, provide an up-to-date picture of CloudIoT applications in literature, to identify open issues, future directions, challenges, and research issues. **Yanmei Hu et al.,2016 [11]** introduces the general issues of multimedia data mining. As per requirement of multimedia data mining, the method of association rules based on cloud computing is discussed with application of Apriori algorithm in cloud computing environment. The accuracy of classical Apriori algorithm and parallel characteristic of mining under the environment of cloud computing, improves the calculation efficiency and speed of data mining. **Majdi Rawashdeh et al.,2016 [12]** presented that the vision of Smart City is realization of efficient models capable of handling huge amount of mobile multimedia data in city's eco-system. Regardless of the improvement in hardware of mobile devices, the issues like: analyzing, managing, and sharing of data still exist. As responsiveness to real time, the applications, bandwidth and wireless constraints can't be achieved by hardware design only. To overcome the challenges, the software side is enabled by Mobile Cloud Computing where parts of mobile applications are executed in remote servers with rich computational resources. Such technology decreases the load on mobile devices and increases their performance. Several models have been proposed to increase the performance and compare them on the basis of several performance parameters, including computation offloading, bandwidth latency, and response time.

The gap in study is bandwidth ratio of more than binary nodes in the cloud media of the client side is minimum gap. The second round of management must be conducted according to the load of work of the streaming node. The streaming nodes have dissimilar hardware specifications and evaluating node.

IV. Scope and Objectives

Multimedia is the field correlated to computer measured integration of texts, graphics, drawings, audio and simulations. The information in the multimedia can be characterized through digitally in contrast to outmoded media. Multimedia technology applies collaborating computer elements such as text, pictures, video, graphics, animation and sound into a single form to deliver the message. Multi-media in cloud computing performances might experimental by individual on phase, projected, communicated, or played close with a media player. A broadcast may be a live or logged multimedia presentation [13].

It is a set of objectives that is associated with a set of objectives that is associated with milestone of this process. The objectives are mentioned below.

1. To study algorithms for encryption and cloud environment for develop approach for securing data on cloud.
2. To implement this mechanism by using the Public Key Cryptography based ARIA (cipher) encryption algorithm and ElGamal key generation scheme.
3. To evaluate the Public Key Cryptography based on ARIA (cipher) encryption algorithm and ElGamal key generation scheme on the basis of some various parameters like encryption time and decryption time.

V. Proposed Algorithm

In this section, we described the proposed algorithm and flow of the implementation of the research work.

5.1 ARIA Algorithm

ARIA is a block cipher with the following characteristics: (i) ARIA quarters key sizes of 128, 192, and 256 bits, and the block size is 128-bit long. (ii) ARIA uses a 16 × 16 evolutional binary matrix with maximum branch number of 8 as its diffusion layer. (iii) ARIA uses the same algorithm for encryption and decryption, taking advantage of its evolutional diffusion matrix. (iv) ARIA is designed to resist many known attacks on block ciphers, including differential cryptanalysis and linear cryptanalysis. (v) ARIA is designed to be efficient both in software and hardware implementations [14]. ARIA is a SPN block cipher with 128-, 192-, and 256-bit keys. It processes 128- bit blocks, and the number of rounds is 12, 14, and 16, dependent on the key size of 128, 192, and 256 bits, individually. The ARIA algorithm can be measured as a series of operations done to 128-bit array called the state. The state is prepared as the plaintext input, and each operation in each round changes the state. The final value of the state is the output of the ARIA algorithm. Most of the processes of ARIA are byte-oriented, therefore occasionally the state is considered as an array of 16 bytes.

5.2 ELGAMAL Algorithm

The ElGamal is based on the security of discrete logarithm issue. To encrypt and distinctly 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 the basis of this software and its problems with ElGamal discovered in late 2003 we will show the vital of correct implementation of cryptographic algorithms [15].

Explanation in proposed work

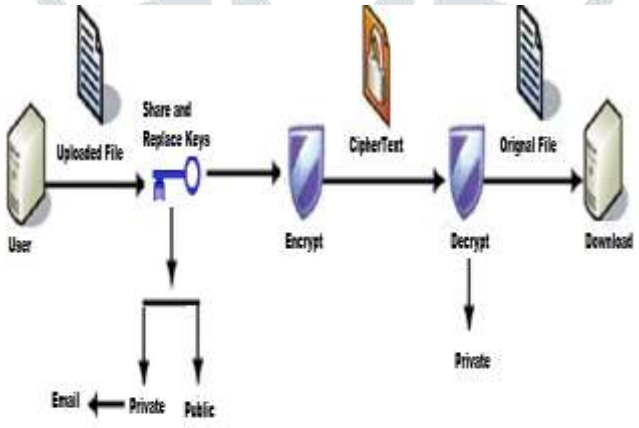

Fig 2. Proposed Flow chart

The process of cryptography in cloud environment with the hybrid approach is used to provide high security for the storage of multimedia content. Various steps are performed by the proposed approach to encrypt the file and provide decryption facility at the time of downloading to the users.

Various steps in this process are as:

User upload file and system create a key using ElGamal algorithm and replace with the actual key of ARIA encryption scheme with the filtration process to make it compatible. This process shares the private key with the user on their email and provide public key to next step for the encryption.

Here system read all bytes of the file and divide it into various sections called block. Divided blocks are process in various iterations and encode the bytes to form a cipher text. This operation performed by the system with public key generated by the ElGamal processing phase. Encrypted data refined by the system and store in the data repository of cloud storage.

Stored data accessed by the user from the corresponding repositories. The system decrypts data with the shared keys and display data elements to users. User can download the files from the server with the use of shared keys on the email for particular file.

.

VI. CONCLUSION

The examination of the information security in cloud cache for multi-media data, which is essentially distributed storage system for more operative and flexible circulated confirmation illustration, to address the data storage security problem in cloud computing, as it relay on the Cryptographic algorithm ELGamal and ARIA to be recycled. These techniques are used for defensive user data include encryption prior to storage user verification measures prior to cache or recovery and structure protected channel for data transmission. This method conserves the obtainability consistency reliability to ensure implied data and at the similar time identifies playful servers. The proposed system expressively recovers the security in cloud computing, Probability Data Access, time and accuracy for multi-media data. The prospect work of planned system focuses on manuscript and imaginary.

REFERENCES

[1] Wang, Shaoxuan, and Sujit Dey. "Adaptive mobile cloud computing to enable rich mobile multimedia applications." *IEEE Transactions on Multimedia* 15, no. 4 (2013): 870-883.

[2] Zhou, Minqi, Rong Zhang, Wei Xie, Weining Qian, and Aoying Zhou. "Security and privacy in cloud computing: A survey." In *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on*, pp. 105-112. IEEE, 2010.

[3] Islam, Mohammad Manzurul, Sarwar Morshed, and Parijat Goswami. "Cloud computing: A survey on its limitations and potential solutions." *IJCSI International Journal of Computer Science Issues* 10, no. 4 (2013): 1694-0814.

[4] Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." *International Journal of Network Security & Its Applications* 6, no. 1 (2014): 25.

[5] Kaur, Er Ramandeep, and Er Gurjot Kaur. "Multimedia Cloud Computing an Emerging Technology: Survey." International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 3 March 2015.

[6] 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, no. 10 (2012): pp-130.

[7] Moens, Marie-Francine, Katerina Pastra, Kate Saenko, and Tinne Tuytelaars. "Vision and Language Integration Meets Multimedia Fusion: Proceedings of ACM Multimedia 2016 Workshop." In *Proceedings of the 2016 ACM on Multimedia Conference*, pp. 1493-1493. ACM, 2016.

[8] Ramesh, B., N. Savitha, and A. E. Manjunath. "Mobile applications in multimedia cloud computing." *International Journal of Computer Technology and Applications* 4, no. 1 (2013): 97.

[9] 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, no. 10 (2012): pp-130.

[10] Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. "Integration of cloud computing and internet of things: a survey." *Future Generation Computer Systems* 56 (2016): 684-700.

[11] Hu, Yanmei, and Mu Yang. "Research on multimedia data mining methods in cloud computing environment." In *Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2016 IEEE*, pp. 752-756. IEEE, 2016.

[12] R. Majdi, A.Alnusair, N. Mustafa, and M. Migdadi. "Multimedia mobile cloud computing: application models for performance enhancement." In *Multimedia & Expo Workshops (ICMEW), 2016 IEEE International Conference on*, pp. 1-6. IEEE, 2016.

[13] Guleria, Sonal, and Dr Sonia Vatta. "To Enhance multimedia security in cloud computing environment using crossbreed algorithm." *International Journal of Application or Innovation in Engineering & Management* 2, no. 6 (2013): 562-568.

[14] Li, Wei, Dawu Gu, and Juanru Li. "Differential fault analysis on the ARIA algorithm." *Information Sciences* 178, no. 19 (2008): 3727-3737.

[15] Erkin, Zekeriya, Alessandro Piva, Stefan Katzenbeisser, Reginald L. Lagendijk, Jamshid Shokrollahi, Gregory Neven, and Mauro Barni. "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing." *EURASIP Journal on Information Security* 2007 (2007): 17.