The Hybrid Approach to Security of Multimedia Data Using Encryption/Decryption and Key Generation Algorithms

Gemini Garg[1], Jaspreet Singh[2]
[1](M.Tech Scholar,Department of IT ,CEC Landran (Mohali), INDIA)
[2] (Assistant Professor,Department of IT,CEC Landran(Mohali),INDIA)
([1]garg.gemini04@gmail.com ,[2]cec.jaspreet@gmail.com)

ABSTRACT: *Cloud Computing has become famous due to its effective characteristics.The growing approval of cloud computing kindsthe data holder to contract complex data in encoded form onto the cloud. Outsourcing the storage and processing of multimedia data to cloud data centres is becoming expanded common. The data in cloud computing is growing producing to scale up the software and hardware resources. How to defend the subcontracted delicate data as a service is becomes a main data safety challenge in cloud computing. According to the safety difficulties that may exist when the users transport the complex data on the network, this paper attempts to improve and specify the operator's encipher processing for the hard data. To deliver rich media services, hypermedia computing has appeared as an important technology to produce, edit, process, and search media insides, such as imageries, audiovisual, acoustic, pictures, and so on. In the research work, this multimedia security problem will be solved by using the mixture of skipjack and Elgamal, Earlier many researchers has work on this topic but none of them archived good accuracy rate, Encryption/Decryption Time and Probability Data Access Rate due to the hybridization.*

Keywords: *Cloud Computing, Multi-media, Security Challenges, Software Resources, Skipjack and Elgamal Algorithm.*

I. INTRODUCTION

Cloud Computing is an expanding popular computing standard, which gives the users considerable computing, storage and software properties on demand. The system Properties are basically shared by numerous users and applications, a perfect task scheduling scenario is difficult to [1] resource utilization and performance of the system. Cloud Computing is recently getting considerable attention in some areas like academic and industrial etc. Cloud computing refers to the distribution of computing resources over the Internet. Instead of possession data on your own hard drive or informing applications for your needs, you use a provision over the Internet, at another location, to store your evidence or use its applications. Doing so may give rise to certain privacy insinuations.

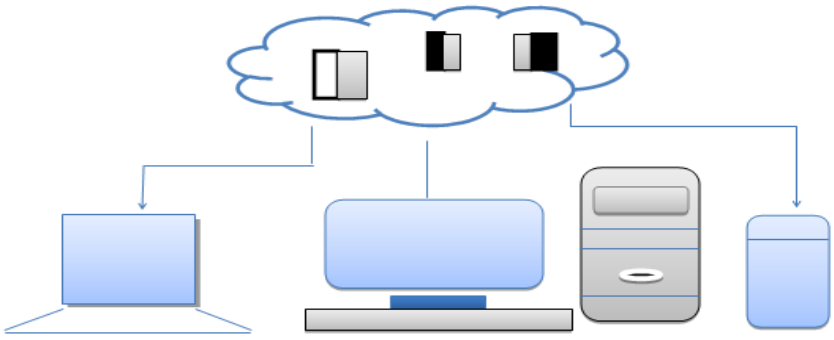


Fig. 1(a): Architecture Cloud Computing

Cloud computing is based on significant principal of reusability the IT capabilities. They are dissimilarity that cloud computing brings comparing to the ancient ideas grid computing, [2] utility computing, dispersed computing or instinctive computing is to the broaden horizons across structure limitations. They data center transform the potential from the capital exhaustive set up to a in consist priced environment.

With many cloud applications being available, maintenance and data security becomes a significant issue in cloud computing. Critical issue in Cloud Computing environments is a data protection or security. The major characteristics of Cloud Computing i.e. Virtualization, Location, Device independence, on-demand Service, Scalability, Resource Pooling and Maintenance.

Clouds Computing are various Advantages are like

- Organization Rate Discount*:* Due to detail that the corporal computing mechanisms that are providing by the cloud, connectivity of the network devices and Main organization costs remain the networking [3] .
- Mobile &social capabilities: The boundless scale is web offers to any application of availability from anywhere and mobility, platform independent. It offers also public declaration facilities to accessible requests, more clients concerned with is therefore making them and providing entrance that our important replicas provide.
- Association & individuality: The cloud permits industries to cooperate with each other easy and to recognize themselves in the market viewpoint. This is one of the main business drivers.

Clouds are three types mentioned in below: i) Public cloud ii) Private cloud and iii)Hybrid cloud

1) Public cloud: In Public Cloud, this is individual and activate by the third party, they are deliver superior finances of the scale to customer, as the infrastructure costs are growth with a mix of the users, mean low cost model an smart the every individual customer an attractive. The security protection, formation, and availability variances are limited customer share the same substructure pool [4].
2) Private Cloud:This model is the managed by an association to provide the control over cloud facilities and organisation. It is assembled to the services within an organization for continuing the security.
3) Hybrid Cloud:The hybrid is also called the virtual private cloud model. It is the mixture both the private and public cloud model. This is achieved by the third-party but some devoted resources are secretly used only by an association.

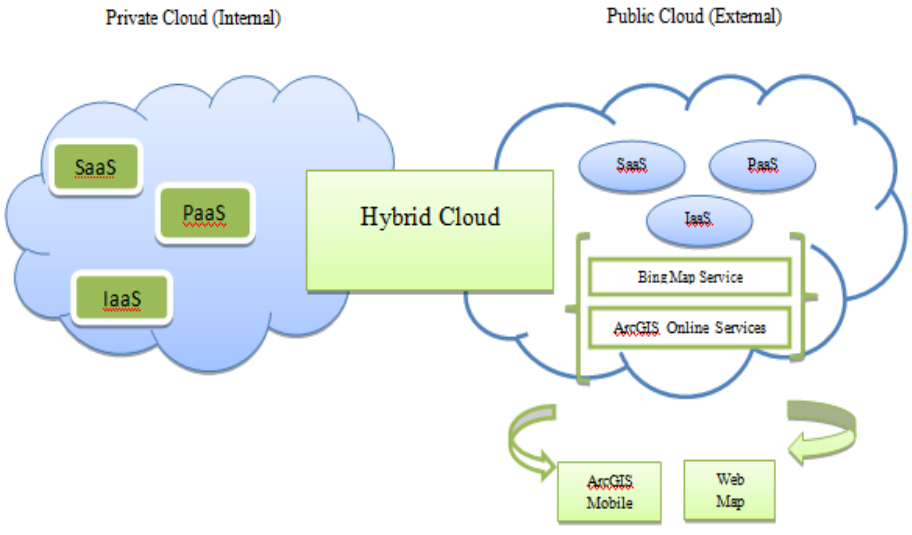


Fig. 1(b): Types of Cloud

II. MULTI-MEDIA CLOUD COMPUITNG

Multi-media are the media uses numerous forms of information content and processing. To enjoying and inform the user. Basically, it refers to the use of electronic media to supply and experience multimedia satisfied. Multimedia is similar to previous mixed media in fine art, but with the broader scope. For programrequests and amenities over the Internet and Mobile Wireless Networks, there are robuststresses for

cloud computing sinceof the important amount of computation required for serving lots of Internet or Mobile Users at the similar time [5].

In this New Cloud founded multi-media dividingmodel, users store and process their multimedia request data in the cloud in a dispersed manner, rejecting full installation of the media request software on the users' processor or device and thus improving the burden of multimedia software maintenance and upgrade as well as careful the computation of user devices and exchangeable the battery of mobile phones.Multimedia processing in a cloud imposes great challenges. Several essential challenges for multi-media computing in the cloud are painted as follows [6]:

1) Service Heterogeneity and Multimedia: As there exist dissimilar types of multi-media and services, such as voice over IP (VoIP), audio-visual conferencing, photo allocation and excision, multi-media streaming, image search, image-based rendering, video trans-coding and variation, and multimedia content delivery, the cloud shall support different types of multi-media and multi-media services for millions of users simultaneously.
2) Network Heterogeneity: As dissimilar networks, such as Internet, wireless local area network and third group wireless network, have different network characteristics, such as bandwidth, delay, and jitter, the cloud shall disseminate multi-media contents for optimal delivery to various types of devices with dissimilar network bandwidths and latencies.
3) Device Heterogeneity: As unrelated types of devices, such as TVs, individual computers and Mobile phones, have dissimilar abilities for multi-media processing, the cloud shall have multimedia edition ability to fit different types of devices, including CPU, GPU, show, memory, storage, and power.

For multi-media computing in a Cloud, concurrent torrents of multimedia data access, processing, and transmission in the cloud would generate a holdup in a general determination cloud because of stringent multimedia QoS necessities and large amounts of users' immediate accesses at the Internet scale. In today's cloud computing, the cloud uses a utility like instrument to allocate how much computing (e.g., CPU) and storage possessions one need, which is very dynamic for general data services.

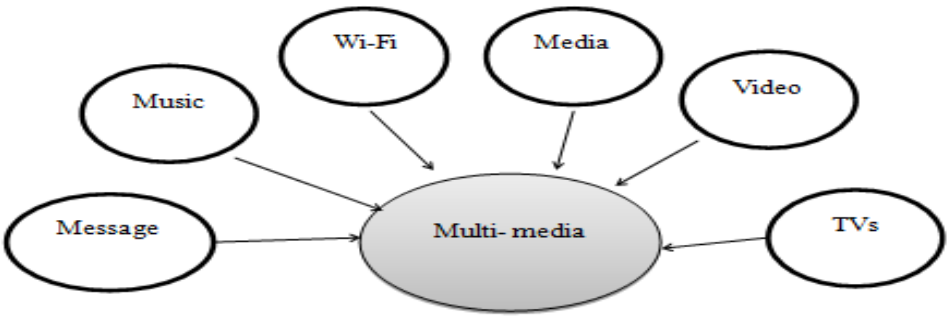


Fig. 2: Overview of Multimedia

III. RELATED WORK

Prof. Radha. S. Shirbhate 2012,[7] Security is necessary for the defense 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 program data. It takes less computational workload and provides five levels of security from level 0 to level 4.

K. Kalaivani et al.,2012,[8] This article, deal with the a variety of techniques connected to safety facet of Multi-media data, particularly the Medicinal data, their compensation and difficulty. The First Part describes the opening of Multimedia data and its use in Medicinal field. The Additional part describes a variety of methods that can be practical for Overall Multi-media data. The third Part defines 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 ultra sonography , positron emission tomography, single photon emission computed tomography , visual imaging , calculated tomography , X-ray, ultrasound, MRI etc.

PravinKawle et al., 2014,[9] 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 unsafe network. Multi-media data safety is reached by methods of cryptography, which deals with encryption of data. Normal symmetric procedures offer improved safety for the multimedia data.

ArokiaSusai Raja Armel et.al.,201310] Studied cloud computing is the existing technology that develop the moveable and IT industry. Greatest of the mobile vendors are if protracted data storage over the cloud either with the third party cloud service worker such as Samsung Android smart headsets with Drop Box storage. On the other hand, Apple iPhone and Openings Phone has their own cloud data storing such as I Cloud and Skydrive respectively. However, mobile phone cloud application users are uncertain to move their data from their mobile earpiece to the cloud service provider because of cumulative data security and privacy concern. In this paper, a moveable data security encryption model is projected to meeting this problem.

IV. PROPOSED TECHNIQUES

Our Proposed Techniques are skipjack and Elgamal Algorithms. Skipjack algorithm used for encryption and Elgamal algorithm used for key generation.

4.1) Skipjack Algorithm: This is a block-cipher established by the Security Agency. It was mainsuggested as the encipher algorithm in a U.S. government supported organisation of key escrow and used only for encryption. Skipjack is a 64-bit code that develops an 80-bit crypto mutable. It encrypts and decrypts 4- 8-bytes of data-blocks, unequal between two sets of treading rules. A Skipjack with full 32 [11] rounds proceed with applying 8 rounds of rule A and 8 rounds of rule B and a repetition of both rules to the plaintext and collecting a total of 32 rounds. In detail, the procedure takes in the input wi k, $1 \leq i \leq 4$.

a) Rule A and B

1) Step of Rule A does the subsequent processes.
   - M Permutes m1.
   - The novel m1 is the logical operation of the M output, the step_counter N and m4.
   - Arguments m2 and m3 shift one location to the right; i.e, become m3 and m4 individually.
   - The novel m2 is the production of M.
   - The step_counter is incremented by one.

2) StepA of Rule B does the subsequent processes.
   - M Permutes m1.
   - The novel m1 is the logical operation of the M output, the stagesecurity N and m4.
   - Words m2 and m3 shift one position to the right; i.e., become m3 and m4 respectively.
   - The novel m2 is the production of M.
   - The step_counter is incremented by 1.

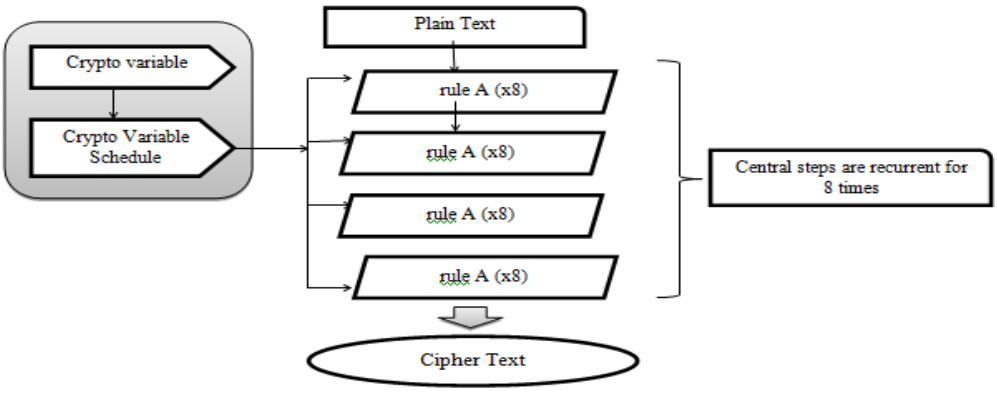


Fig. 4: Skipjack Algorithm (Encryption)

4.2) Elgamal Algorithm

The ElGamal Algorithm is a public-key Cryptosystem created on the discrete log difficulties. It contains of both encryption and sign algorithms. The encryption algorithm is similar in nature to the diffie-hellman Key Agreement rules.

A. Generating the Key

- Select a large prime number a, such that (a-1)/2 is prime, too. D is the number of bits of a [12].
- Select the base alpha<a.
- Select the private key b<a.
- Compute beta = alpha^{a} (mod a).
- Publish a, alpha and beta as public key.

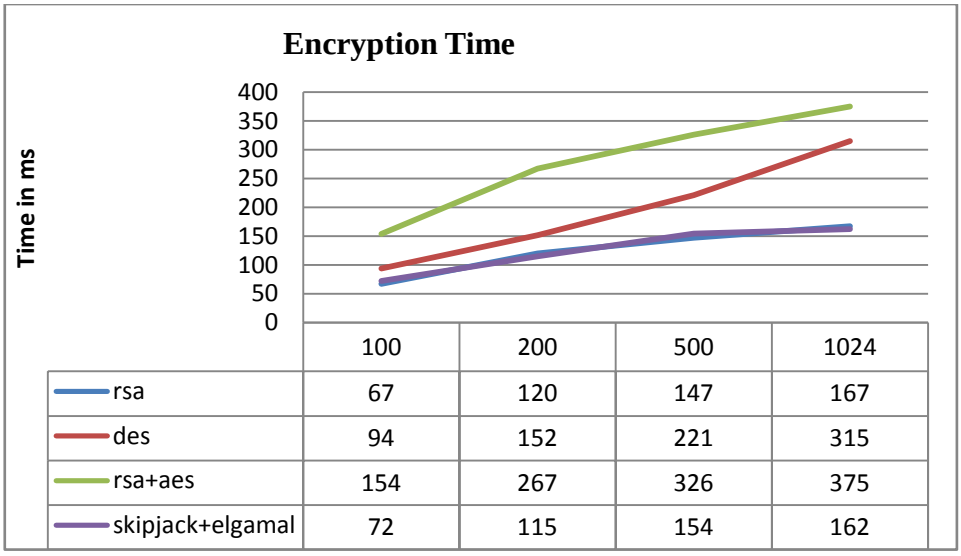
B. Encryption of Message

- Separate the plaintext into blocks of D-1 bits.
- Select a secret random number b with gcd(b,a-1)=1.
- Compute for every block c the ciphertext e(c,b) = (y1,y2) … where y1 = alpha^{b}(mod a) and y2 = beta^{b}c (mod a).y1 and y2 are blocks of the length D of ciphertext.

C. Decryption of a Message

- Separate the ciphertext in blocks of D bits
- For two successive blocks y1 and y2 solve y1^{a}c = y1(mod a) for x. Thus d(y1,y2) = x= y2(y1 ^{a})$^{-1}$ (mod a) is the wanted block of plaintext.

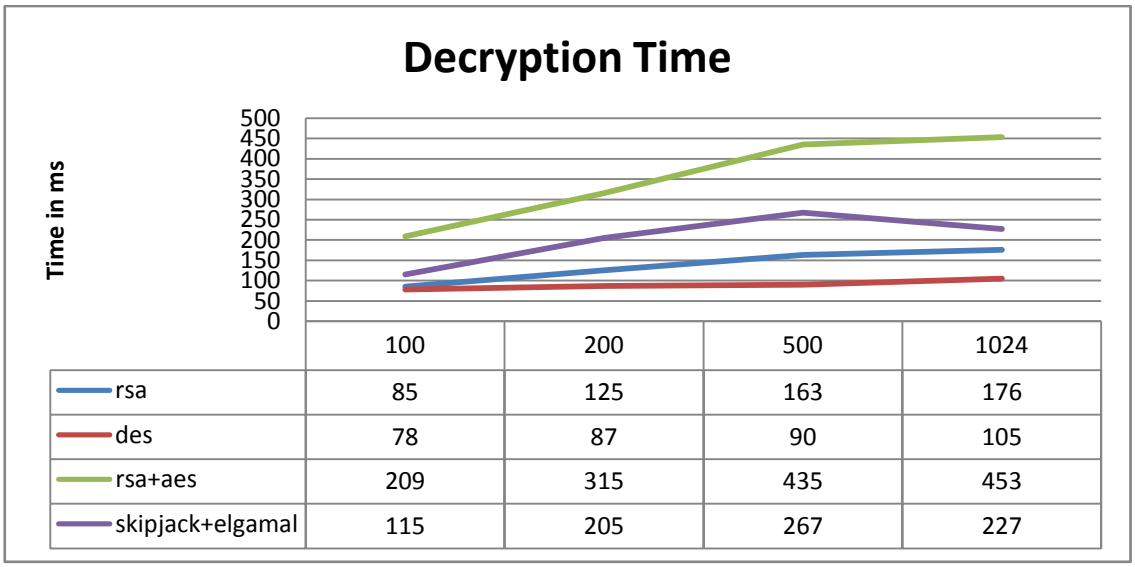
V. COMPARISON RESULTS



	100	200	500	1024
rsa	67	120	147	167
des	94	152	221	315
rsa+aes	154	267	326	375
skipjack+elgamal	72	115	154	162

Fig. 5: Encryption Time

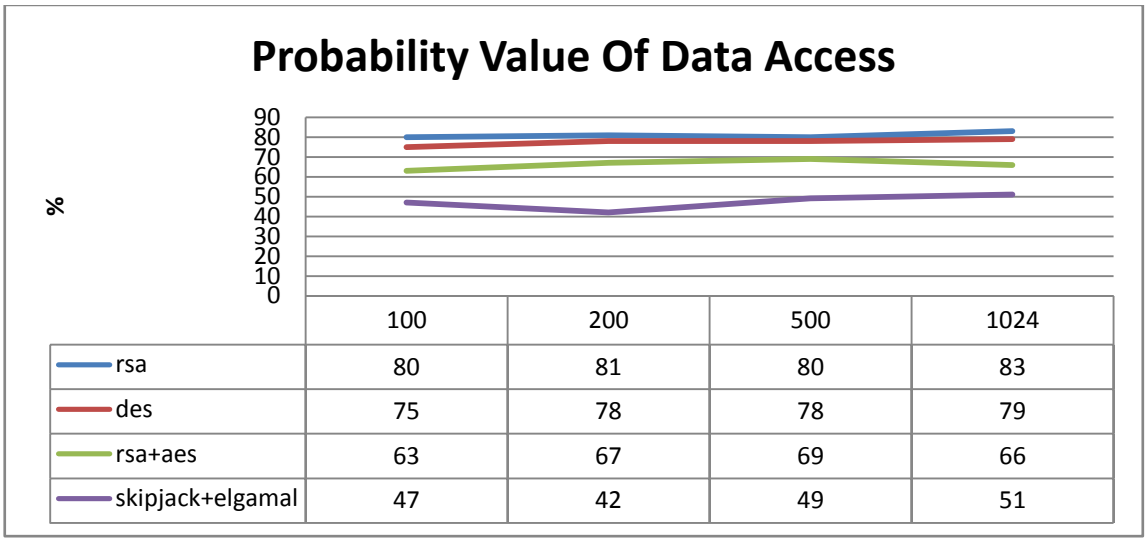
Encryption time shows the time consumption of hybrid and other algorithm. It's a total time consumption that particular algorithm takes during convert normal file into cipher text. The hybrid algorithm shows better results in this graph during file encryption.



	100	200	500	1024
rsa	85	125	163	176
des	78	87	90	105
rsa+aes	209	315	435	453
skipjack+elgamal	115	205	267	227

Fig. 6: Decryption Time

Decryption time is another parameter which is a total time consumption taken by algorithm to extract original content from cipher text. The comparison with other algorithm the hybrid algorithm will take little more time than other single algorithm because it's a much secure process and combination of two different algorithms but will perform better than other hybrid algorithm.



	100	200	500	1024
rsa	80	81	80	83
des	75	78	78	79
rsa+aes	63	67	69	66
skipjack+elgamal	47	42	49	51

Fig. 7: Probability Value of Data Access

Probability parameter used to detect the security factor of a particular system. This parameter shows the possibility of access file from a secure system. The hybrid algorithm performs better result in this process with compare to other algorithms.

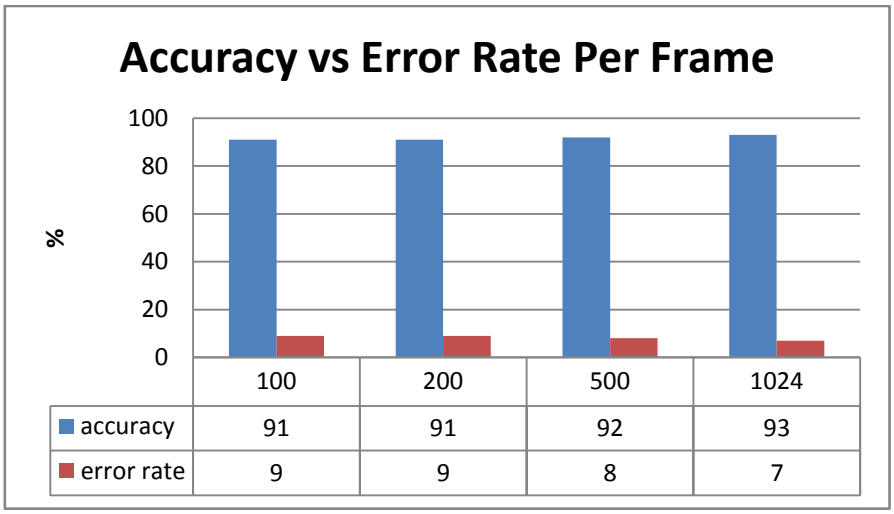


Fig. 8: Accuracy vs Error Rate Per Frame

This Graph shows the two parameters accuracy and error rate per frame when we convert cipher to original mode of a file. These values show consistent result with multiple executions on different file size.

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 circulatedconfirmationillustration, to address the data storage security problem in cloud computing, as it relay on the Cryptographic algorithm ELGamal and Skipjack to be recycled. These techniques are used for defensive user data include encryption prior to storage user verificationmeasures prior to cache or recovery and structureprotected channel for data transmission. This method conserves the obtainabilityconsistencyreliability to ensure implied data and at the similar time identifies playful servers. The proposed system expressivelyrecovers 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] Li, Jin. "Identity-based encryption with outsourced revocation in cloud computing." *Computers, IEEE Transactions on* 64.2 (2015): 425-437.
[2] Kehoe, Ben, "A survey of research on cloud robotics and automation", *Automation Science and Engineering, IEEE Transactions on* 12.2 (2015): 398-409.
[3] Carroll, Mariana, Alta Van Der Merwe, and Paula Kotze, "Secure cloud computing: Benefits, risks and controls", *Information Security South Africa (ISSA), 2011*, IEEE.
[4] Buyya, Rajkumar, et al., "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", *Future Generation computer systems* 25.6 (2009): 599-616.
[5] Wang, Shaoxuan, and SujitDey, "Adaptive mobile cloud computing to enable rich mobile multimedia applications", *Multimedia, IEEE Transactions on* 15.4 (2013): 870-883.
[6] Islam, Salekul, and Jean-Charles Grégoire, "Giving users an edge: A flexible Cloud model and its application for multimedia", *Future Generation Computer Systems* 28.6 (2012): 823-832.
[7] Islam, Salekul, and Jean-Charles Grégoire, "Giving users an edge: A flexible Cloud model and its application for multimedia", *Future Generation Computer Systems* 28.6 (2012): 823-832.
[8] Kalaivani, K., and B. Sivakumar, "Survey on multimedia data security", *International Journal of Modeling and Optimization 2.1* (2012): 36-41.
[9] Kawle, Pravin, "Modified Advanced Encryption Standard.", *International Journal of Soft Computing and Engineering, Vol. 4 (1),* March 2014.
[10 Armel, ArokiaSusai Raja, and V. Thavavel., "Ghost encryption: Mobile data security model encrypting data before moving it to the cloud service provider", Advanced Computing (ICoAC), *Fifth International Conference on.IEEE,* 2013.
[11] Kong, JiaHao, "Low-complexity two instruction set computer architecture for sensor network using Skipjack encryption", *Information Networking (ICOIN), International Conference on*.IEEE, 2011.
[12] Sharma, Prashant, Sonal Sharma, and Ravi Shankar Dhakar, "Modified Elgamal Cryptosystem Algorithm (MECA)", *Computer and Communication Technology (ICCCT), 2nd International Conference on*.IEEE, 2011.