ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

An Analytical Review of the Multimedia Data and Encryption Mechanism at Cloud Server

Aafaq Ahmad Peerzada[1], Er.Rishma Chawla[2]

M.Tech Scholar, Dept. of Computer Science and Engineering, RIET Phagwara Punjab, India[1]

Professor, Dept. of Computer Science and Engineering, RIET Phagwara Punjab, India[2]

ABSTRACT: Cloud computing is an emerging style of IT delivery that intends to make the Internet the ultimate home of all computing resources- storage, computations, and accessibility. The next generation architecture of IT Enterprise is envisaged in Cloud Computing because of its robustness, scalability, performance, high availability, least cost and many others. The delivery of Services by cloud Service Providers is hampered because of the security concerns shown by the Enterprises and vendors as the cloud environment gives access to centralized shared hardware, software and other information. The security issues in cloud computing such as service availability, massive traffic handling, application security, and authentication. The focus of this paper would be to cover secured storage and access methods of multimedia content over the content delivery cloud edge servers. This paper also focuses on the encryption mechanism like Blow Fish, DES and the control mechanism like CHAP.

KEYWORDS: Cloud Computing, Security Algorithms, Cryptography, Multimedia, Modified Blow fish, DES, CHAP authentication, Digital Signature.

I. INTRODUCTION

Cloud Computing fulfills long term dream of computing as a utility and thus represents an inflection point in the geography of computation and IT services delivery. Cloud computing multimedia database is based on the current of database development, object-oriented technology and object-oriented fields in the database, which increasing display its vitality [1]. Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction[2]. Cloud computing provides a computer user access to Information Technology (IT) services i.e., applications, servers, data storage, without requiring an understanding of the technology or even ownership of the infrastructure.

To comprehend cloud computing, an analogy to an electricity computing grid is to be useful. A power company maintains and owns the infrastructure, a distribution company disseminates the electricity, and the consumer merely uses the resources without the ownership or operational responsibilities receiving a great deal of attention, both in publications and among users, from individuals at home to the U.S. government. Cloud computing is a subscription-based service where you can obtain networked storage space and computer resources. a user's cloud computing access enables "shared resources, software, and information on-demand on a fee-for-service basis[4]. According to the National Institute of Standards and Technology (NIST), cloud computing exhibits several characteristics: Agility improves with users' ability to re-provision technological infrastructure resources [5]

Delivery Models

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider (e.g., java, python, .Net). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but the consumer has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to rent processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers).

Deployment Models

Private cloud: The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

Public cloud: The cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group.

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (internal, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting). Each deployment model instance has one of two types: internal or external. Internal clouds reside within an organizations network security perimeter and external clouds reside outside the same perimeter.

There are many types of public cloud computing:

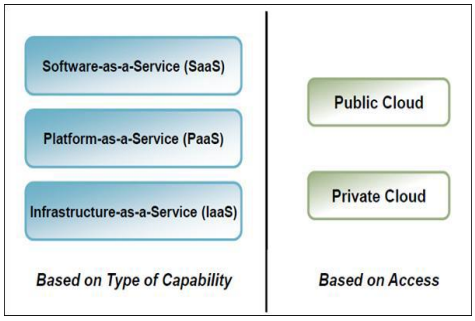


Figure 1. General Architecture of Cloud

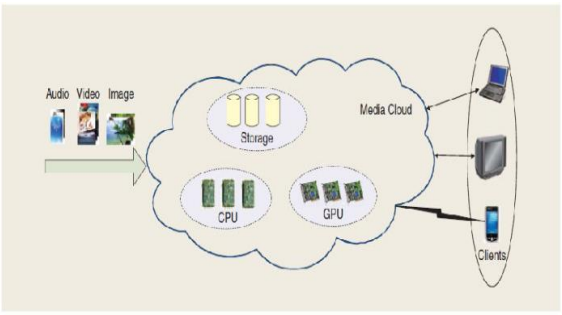


Figure 2. Overview of Multimedia system in Cloud

MULTIMEDIA SYSTEM: Internet multimedia is emerging as a service with the development of Web 2.0. Multimedia computing has emerged as a noteworthy technology to generate, edit, process, and search media contents, such as images, video, audio, graphics, and so on which provide rich media services as shown in figure 1.2. For multimedia applications and services over the Internet and mobile wireless networks, there are strong demands for cloud computing because of the significant amount of computation required for serving millions of Internet or mobile users at the same time [4]. In new cloud-based multimedia-computing paradigm the users store and process their multimedia application data in the cloud in a distributed manner, eliminating full installation of the media application software on the users' computer or device and thus alleviating the burden of multimedia software maintenance and upgrade as well as sparing the computation of user devices and saving the battery of mobile phones. Multimedia processing in a cloud imposes great challenges. Several fundamental challenges for multimedia computing in the cloud are highlighted as follows [5].

Multimedia and service heterogeneity: The types of multimedia and services, such as voice over IP (VoIP), video conferencing, photo sharing and editing, multimedia streaming, image search, image-based rendering, video

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

transcoding and adaptation, and multimedia content delivery, the cloud shall support different types of multimedia and multimedia services.

QoS heterogeneity: For different multimedia services different QoS requirements should be include and the cloud shall provide QoS provisioning which support for various types of multimedia services to meet different multimedia QoS requirements.

Network heterogeneity: The cloud shall adapt multimedia contents for optimal delivery to various types of devices with different network bandwidths and latencies which providing different networks, such as Internet, wireless local area network (LAN), and third generation wireless network, have different network characteristics, such as bandwidth, delay, and jitter.

Device heterogeneity: As different types of devices, such as TVs, personal computers (PCs), and mobile phones, have different capabilities for multimedia processing; the cloud shall have multimedia adaptation capability to fit different types of devices, including CPU, GPU, display, memory, storage, and power. A computer system with the capabilities to capture, digitize, compress, store, decompress and present information is called multimedia system. The aim of multimedia system is to provide a creative and effective way of producing, storing and communicating information. The application areas of multimedia are marketing, training, education, entertainment, etc.

II. 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), 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 Cloud Front, 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 Cool stream.

Wenwu Zhu [5] presented the fundamental concept and a framework of multimedia cloud computing. They addressed multimedia cloud computing from multimedia-aware cloud and cloud-aware multimedia perspectives. On the multimedia-aware cloud, they presented how a cloud can provide QoS support, distributed parallel processing, storage, and load balancing for various multimedia applications and services. Specifically, they proposed an MEC-computing architecture that can achieve high cloud QoS support for various multimedia services. On cloudaware multimedia, we addressed how multimedia services and applications, such as storage and sharing, authoring and mashup, adaptation and delivery, and rendering and retrieval, can optimally utilize cloud-computing resources.

Jiann-Liang Chen [6] proposed a novel IP Multimedia Subsystem (IMS) framework with cloud computing architecture for use in high quality multimedia applications. The IMS supports heterogeneous networking with Quality-of-Service (QoS) policy. Map Reduce analysis is also used to enhance cloud computing capability. This architecture enables users to access high-quality multimedia applications via Android-based appliances. In this study, the IMS QoS policies of three wireless access technologies, 3G, Wi-Fi and Wi-MAX, are integrated in a cloud computing environment to provide different services such as VoIP services and video streaming services. Experimental results indicate that the proposed mechanism improves system performance by allocating resources according to service priority. The proposed architecture also significantly improves system capacity to accommodate numerous users. The proposed IMS Cloud QoS mechanism has the following three layers: Infrastructure as a Service (IaaS) layer, Platform as a Service (PaaS) layer, and Software as a Service (SaaS) layer. The IaaS layer mainly accesses heterogeneous networks such as UMTS, WLAN and WiMAX through the IP Multimedia Subsystem, which utilizes the QoS policy module to achieve high quality service, and the core network as the cloud computing data center. The PaaS layer manages the cloud computing system in the Hadoop Distributed File System and the Map Reduce mechanism for analyzing user preferences. The SaaS layer allows users to access desired applications such as the Web, social networks and management services. The system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

implementation shows that throughput capacity with cloud computing is higher than without cloud computing when numerous users request services. It also improves system throughput performance.
Li Li [7] elaborates the environment, the necessity of information integration, technical support and the method of integration under the environment of cloud computing, and is aimed to figure out the way to establishing operational mechanisms to achieve integration of distributed heterogeneous data sources and integration and transparency of location, structure, semantic of enterprise heterogeneous data, and solve the issue of comprehensive sense, resource allocation, and timely response on service integration and sharing of resources effectively.
Tamleek Ali [26] proposed a framework for the use of cloud computing for secure dissemination of protected multimedia content as well as documents and rich media. They have leveraged the UCON model for enforcing fine-grained continuous usage control constraints on objects residing in the cloud. Their framework allows for the object owner to specify his/her policies regarding usage of the protected objects ensuring the enforcement of his/her policies including those specifying say, the duration of each use, the number of times the object can be used etc.

III. DATA SECURITY ISSUES IN THE CLOUD

Privacy and Confidentiality: Once the client host data to the cloud there should be some guarantee that access to that Data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.
Data integrity: With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.
Data Location and Relocation: Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want o know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server.
Data Availability: Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.
Storage, Backup and Recovery: When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers.. Security in data storage is one of the most important metrics in performance comparison of these cloud computing systems. If the provided cloud storage can be accessed or destroyed by malicious attackers, the service provider will lose trust from its users, and the leakage of personal data could cause great damage to each individual. Storage Security consists of:

- Physical Storage Security
- Data Security

IV: PROPOSED ALGORITHMS

DES Algorithm: It is a symmetric encryption system that uses 64-bit blocks, 8 bits (one octet) of which are used for parity checks (to verify the key's integrity). Each of the key's parity bits (1 every 8 bits) is used to check one of the key's octets by odd parity, that is, each of the parity bits is adjusted to have an odd number of '1's in the octet it belongs to. The key therefore has a "useful" length of 56 bits, which means that only 56 bits are actually used in the algorithm. The algorithm involves carrying out combinations, substitutions and permutations between the text to be encrypted and the key, while making sure the operations can be performed in both directions (for decryption). The combination of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

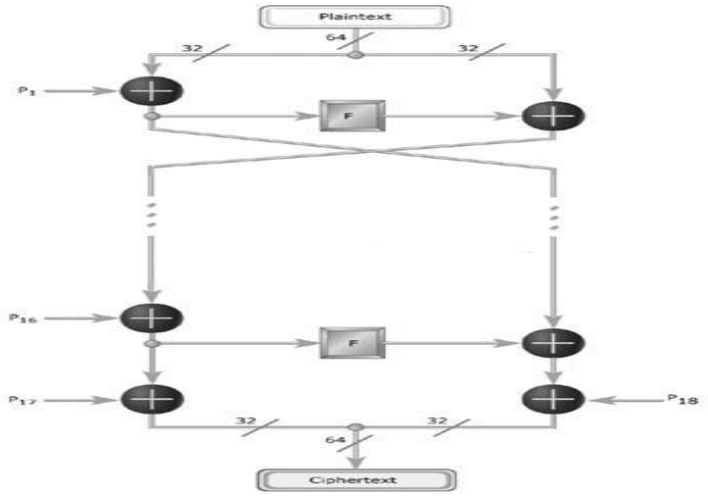
(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

substitutions and permutations is called a product cipher. The key is ciphered on 64 bits and made of 16 blocks of 4 bits, generally denotedk1 to k16. Given that "only" 56 bits are actually used for encrypting, there can be 256 (or 7.2*1016) different keys!

The main parts of the algorithm are as follows:

- Fractioning of the text into 64-bit (8 octet) blocks;
- Initial permutation of blocks;
- Breakdown of the blocks into two parts: left and right, named L and R;
- Permutation and substitution steps repeated 16 times (called rounds);
- Re-joining of the left and right parts then inverse initial permutation.



.

Figure 3. DES Algorithms steps

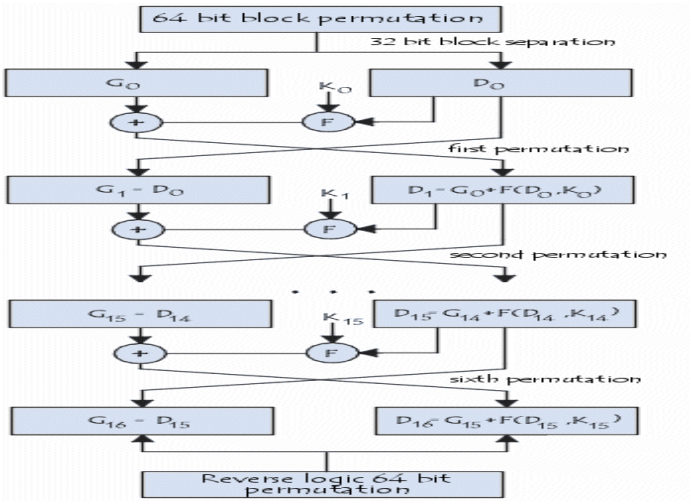


Figure 4. Representation of Blowfish Algorithm.

Key Generation	
Select p, q	p, q both prime, p≠q
Calculate n = p×q	
Calculate $\phi(n) = (p-1)\times(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1<e<\phi(n)$
Calculate d	
Public key	KU = {e, n}
Private key	KR = {d, n}

Encryption	
Plaintext:	M < n
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Figure 5. The RSA Algorithm Flow.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

BLOW FISH: Blowfish cryptographic algorithm [24], which was designed by Bruce Schneier in 1993, is a symmetric block cipher that divides a message up into fixed-length blocks of 64-bit during encryption and decryption processes, as shown in Figure 1. The Blowfish algorithm consists of two parts: a key expansion part and a data-encryption part. Key expansion converts a variable-length key of at most 448 bits into several subkey arrays, totaling 4168 bytes. The algorithm uses Feistel cipher where the input text is split into two halves. The first half is applied round function using a subkey. The output will be XORed with the second half. Then the two halves will be swapped. In total there are 17 rounds and each round consists of a key-dependent permutation and a key- and data-dependent substitution. Hence, this serves as the candidate in our pipelined model. By the end of the 17th round, the 64-bit cipher text will be produced [17]. The Feistel network of Blowfish algorithm is one that utilizes a structure that makes encryption and decryption very similar through the use of the following elements [3, 18]:

- P-box: Permutation box that performs bit shuffling;
- S-box: Substitution box for non-linear functions;
- XOR: Logic function to achieve linear mixing.

The RSA Algorithm: The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secures public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers. Using an encryption key (e,n), the algorithm is as follows:

1. Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the eth power modulo n. The result is a ciphertext message C.
3. To decrypt cipher text message C, raise it to another power d modulo n

The encryption key (e,n) is made public. The decryption key (d,n) is kept private by the user.
How to Determine Appropriate Values for e, d, *and* n

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as p and q.
2. Set n equal to $p * q$.
3. Choose any large integer, d, such that GCD(d, ((p-1) * (q-1))) = 1
4. Find e such that $e * d = 1$ (**mod** ((p-1) * (q-1)))

Rivest, Shamir, and Adleman provide efficient algorithms for each required operation[8].

IV. PROBLEM FORMULATION

The existing frameworks proposed so far focuses only on securing the data stored either on the distributed servers or local servers interacting with cloud through interfaces or agents. The use of either applying the encryption algorithms or putting the authentication mechanism inplace alone cannot help to protect the data from the unauthorized access keeping in view the preset robust attacking models. So the need is to suggest such a mechanism where encryption of the content, authorization of user as well the delivery of content to end terminals has been considered.

V. PROPOSED MODEL

In this model we will explore the ways to enhance the security of multimedia content using hybrid algorithms while being delivered to their end users. The security frame work will take care of authorization and authentication of user

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

while accessing any cloud server. The hybrid encryption mechanism will make the storage and transmission secure by associating some payloads defining the minimum required security parameters. The robustness of this delivery mechanism will cover the multimedia streaming over CDC, caching the media content onto the edge server from storage cloud and will be used to minimize the latency of content delivery. The overall scenario will outline architecture for designing and deployment of Applications with rich multimedia content over cloud servers as SAAS and also taking the advantage of blob storage of clouds like Windows azure which provide ready to use services like

- Serving images or documents directly to a browser
- Storing files for distributed access Streaming video and audio
- Performing secure backup and disaster recovery
- Storing data for analysis by an on-premises or Windows Azure-hosted service

VI. CONCLUSION

The Cloud computing as a technology would be adopted if the areas of concerns like security of the data will be covered with full proof mechanism. The strength of cloud computing is the ability to manage risks in particular to security issues. Our suggested model will present an outline sketch of architecture to be adopted by architects involved in implementing the cloud computing. Security algorithms mentioned for encryption and decryption and ways proposed to access the multimedia content can be implemented in future to enhance security framework over the network. In the future, we will try to explore our research by providing algorithm implementations and producing results to justify our concepts of security for cloud computing.

REFERENCES

[1]. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia (2009, Feb. 10). Above the clouds: A Berkeley view of cloud computing. EECS Dept. University of California, Berkeley, No.UCB/EECS-2009-28[Online].Available: http://radlab.cs.berkeley.edu/

[2]. NIST-Draft-SP-800-144_cloud-computing

[3]. D. Parkhill. The Challenge of the Computer Utility.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

[4] 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.

[5]. 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.

[6]. Jiann-Liang Chen, Szu-Lin Wu, Yanuarius Teo filus 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.

[7] Li Li, Xiong Li, Sun Youxia, and Liu Wen; "Research On Mobile Multimedia Broadcasting Service Integration Based On Cloud Computing". Multimedia Technology (ICMT), 2010 International Conference on 29-31 Oct. 2010, 10.1109/ICMULT.2010.5630979, 1-4

[8]. Pekka Riikonen, "RSA Algorithm", 2002

[9] 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.

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

[11] http://news.wxiu.com/200907/27-6135.html.

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

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

[14].Sunguk Lee. Research Institute of Industrial Science and Technology Pohang, Gyeongbuk, South Korea

[15].Balakarishnan.S,Saranya.G,Shobana.S,rthikeyan.S "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", IJCST Vol.2, Issue 2, June 2011.

[16] Joshi Ashay.M et al, "Enhancing Security in Cloud Computing", ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 1, No.1, 2011

[17] Richard Chow, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, Yuan Niu, Elaine Shi, Zhexuan Song. "Authentication in the Clouds: A Framework and its Application to Mobile Users", CCSW'10, October 8, 2010, Chicago, Illinois, USA.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

[18] Honywei Li, Yuanshun Dai, Bo Yang. "Identity-Based Cryptography for Cloud Security".
[19] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing. "Data Security Model for Cloud Computing", ISBN 978-952-5726-06-0, Qingdao, China, November 21-22, 2009.
[20] Qiu Xiu-feng, Liu Jian-Wei, Zhao Peng-Chuan. "Secure Cloud Computing Architecture on Mobile Internet", IEEE-2011.
[21] Mayayuki Okuhara, Tetsuo Shiozaki,Takuya Suzuki."Security Architectures for Cloud Computing", 2009.
[21] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing , Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) , ISBN 978-952-5726-06-0.
[23].http://www.guardian.co.uk/technology/blog/2010/sep/21/twitter-bug- malicious- exploit
[24]. Manikandan Ganesan, Krishnan Ganesan, "A Novel Approach to the Performance and Security Enhancement Using Blowfish Algorithm", *International journal of Advanced Research in Computer Science, 2011.*
[25].William Stallings, Cryptography and Network Security, 3rd Ed, Wiley, 1995.
[26]. Tamleek Ali, Mohammad Nauman, Fazl-e-Hadi, "On Usage Control of Multimedia Content in and through Cloud Computing Paradigm, 978-1-4244-6949-9/10/$26.00 ©2010 IEEE.

BIOGRAPHY

Aafaq Ahmad Peerzada is M. tech Research Scholar Department of Computer Science and Engineering , RIET Phagwara Jalandhar, Punjab India. His research interests are Cloud computing and security, information security, wireless Networks, Enterprise computing, Algorithms, web 2.0 etc .

Professor Er.Rishma Chawla is Heading the Dept of 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 security, information security, Data mining wireless Networks.