International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Efficient and Secure Data Storage in Cloud Computing Through Blowfish, RSA and Hash Function

Nirmaljeet Kaur[1], Harmandeep Singh[2]

Department of Computer Engineering, Punjabi University Patiala, Punjab, India

Abstract: ***Cloud computing is the way of providing computing resources in the form of services over internet. The cloud computing allows storing the user's data and to measure the applications and services provided by cloud server. There is an ample data stored at cloud storage server. Security is one of the major issues which reduces the growth of cloud computing So Cloud computing entails encyclopedic security solutions .This paper presented secure file exchanging on Cloud using Blowfish, RSA and Hash algorithms which is capable of solving data security, authentication, and integrity problems of files on the cloud. Data security is improved by cryptography algorithms. The rightness of data is verified by introducing Hash techniques. Enhanced system (Blowfish+RSA+Hash value) compares with simple RSA and Blowfish on basis of some performance parameters like:- throughput, encryption time ,cipher text and delay time . In our enhanced system we integrate symmetric, asymmetric and Hash algorithms which provide better results for performance parameters .TPA which has to match the Hash code for the integrity of user data in cloud on behalf of Data Owners. Data Owner can get notification from TPA when the data integrity is lost.***

Keywords: cloud storage server, cloud computing , TPA.

1. Introduction

Cloud computing[13] is defined as for enabling suitable, on-demand network entrance to a shared pool of configurable calculating resources .Cloud computing consists

- Elasticity &Scalability
- Pay-as-you-use.
- Standardization
- Provisioning

Cloud computing is the next generation in computation. Cloud is a style of computing in which
IT-related capabilities are provided "as a service", allowing users to access technology-enabled services from the Internet (i.e., the Cloud) without knowledge of, expertise with, or control over the technology infrastructure that supports them. Email was probably the first service on the "cloud".

In cloud computing, everything is delivered as a Service (XaaS). There are three main service models such as:

- Software as a Service (SaaS).
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS

Four deployment models [1] of cloud are as: Public Cloud: Cloud computing in which infrastructure is available to the general public and offered services are made available to anyone, from anywhere and anytime through internet. Private Cloud: Cloud infrastructure is operated for a private organization. It may be managed by a third party or by the organization .Hybrid Cloud: Cloud infrastructure is combination of heterogeneous clouds (private, public and community clouds).Community Cloud: Cloud infrastructure supports a specific community (security requirements, policy and mission etc.)

A. Security Issues

Cloud has many challenging design issues which demand great knowledge affecting on the security and performance of the overall system. Many security issues [18] are:

- Data Security [17]: Traditionally sensitive data stored within organization boundary, but in cloud enterprise data is stored outside the enterprise boundary, which required strong encryption.
- Cloud Privacy and Confidentiality: Confidentiality is defined as the sensitive data is not disclosed to unauthorized process, devices and person .cloud service provider knows where the user's private data located in the cloud.
- Data location and relocation [13]: cloud storage is black box. Consumers always don't know the location of their data. Cloud computing offers high degree of data mobility.
- Storage, Backup and Recovery [17]: When customers move their data on cloud the cloud service provider ensure adequate data resilience storage system. Cloud storage providers will manage the data in multiple copies across many independent locations.
- Data Integrity [17]: Data integrity is the rightness of data stored at cloud. The alterations between two updates of a data record violate the data integrity.

To resolve these security issues many cryptography algorithms available. Cryptography[5] can provide services, such as:integrity checking—reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source and authentication .Secure the cloud means secure the storage database hosted by the cloud provider. Security goals achieved by encryption /decryption process [10] Encryption/Decryption process are combination of three types of algorithms:

1. Symmetric Key: Symmetric key cryptography refers to encryption methods in which both the sender and receiver share the same key [15]. In symmetric key cryptography; the same key is used by both parties. For example:- DES, AES, 3DES, BLOW FISH etc.

2. Asymmetric Key: Public key cryptography, where different keys are used for encryption and decryption[18]. In asymmetric or public key cryptography, there are two keys: a private key and a public key are used. The private key is kept by the receiver and public key is announced to the public. For example :- RSA, Diffie Hellman, DSA .

3. Hash Algorithms: A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography"[14]. The input data is often called the message, and the hash value is often called the *message digest* or simply the *digest*.For example:- MD5,SHA etc.

To ensure the correctness of users 'data in the cloud, we propose an effective mechanism with salient features of data integrity, confidentiality and authentication. This mechanism uses the concept of Blowfish, RSA along with Hash function. Hash function improves the file integrity. We compute Hash at client side and compare this hash function value at TPA server as well as main server. In this scheme encryption is used to provide security to the data while in transmit. Because the encrypted file is stored on the cloud, so user can believe that his /her data is secure. Only in encrypted form of files transferred over the channel, which reduces the problem of information disclosure.

Our enhanced system (Blowfish+RSA+Hash value) compares with simple RSA and Blowfish on basis of some performance parameters like:- throughput, encryption time ,cipher text and delay time .

This paper mainly concern with the introduction of cloud computing, security issues related to cloud and some basics techniques available for integrity of data in cloud server. First section covers the introduction of cloud computing and security issues related to cloud. Second section of paper covers some related work or techniques performed for proof of storage. Third section consists introduction of Blowfish ,RSA and SHA algorithms. Fourth section covers the proposed methodology and fifth section covers the result of comparison between blowfish, rsa and proposed system. Last section of paper we conclude the better security algorithms for integrity in cloud.

2. Related Work

Cloud supports large volume of data at cloud storage. But in Cloud Computing there are many pressures which are avoiding the wide receipt of cloud .One of the main threats is data confidentiality and data integrity in cloud storages. There is lot of research going on in this field to ensure and provide data integrity in cloud storages. Calce introduces about cloud computing putting everything into single box will only make it easier for hackers [10]. Priya Metri and Geeta Sarote introduce threat model to treat privacy problems in the cloud [12]. One of the biggest concerns with cloud data storage is that truth verification of cloud data at untrusted server. For high efficiency & retrievability of data required a verifier i.e. TPA. Third Party Auditing notify threats in cloud computing is tampering the data in cloud that interfere with unauthorized modification for data, which lead to an effectiveness processors, data storage and data flow. Dalia Attas, Omar Batrafi implemented a mechanism in which integrity is checked at 2 sides- by cloud server (for inside attack) and by TPA (for outside attack) using digital signature with MD5 [8]. Juels and Kaliski proposed a model Proofs of Retrievability (POR) to formulize the notion "guaranteed remotely and reliable integrity of the data without retrieving of data file"[1]. Sravan Kumar et al. proposed a method of proof by adopting the use of Meta data. Meta data is created using randomly selected bits from original data file and is appended in an encrypted form to be stored on cloud. Whenever verifier wants to check integrity, he throws a challenge by specifying block number and its corresponding Meta data and finally decrypted for proof of correctness[16].Waters and Shacham present a new model for POR enabling verifiability of data without access the entire file and reduced overhead [6].

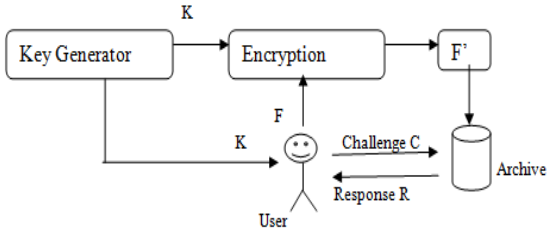

Figure 1: Schematic view of a proof of retrievability based on inserting random sentinels in the data file [1]

Paresh D.Sharma et al. proposes use the symmetric key technique AES cryptography algorithm for stored data as well as for the data that are moving within the cloud or for outsider service provider. Then this service provider can't use these data if it didn't get the key of cryptography. So the service provider in the cloud should use the key to get & use these data [11].Ms.Payal P.Kilor et. Proposed a model to avoid TPA, so the integrity check of data stored in cloud at customer's side using security keys [9].

3. Blowfish

Blowfish is an encryption algorithm[3] that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric block cipher that uses a variable length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use. Blowfish cryptographic algorithm [5],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. The Blowfish algorithm consists of two parts[7]: 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.

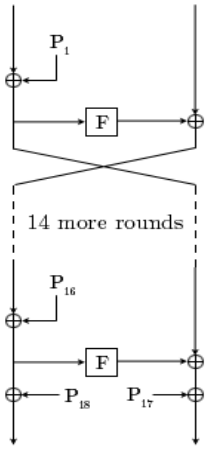

Figure 3: Representation of Blowfish Cryptographic Algorithm

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 [2, 17]:

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

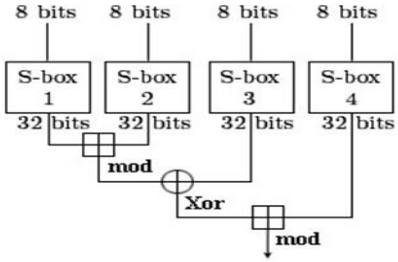

Figure 1: Representation of F function

Figure[3] shows a graphical representation of the F function,which has been shown as the most accessed function of the Blowfish algorithm. It requires a 32 bit input data to be decomposed into four 8 bit blocks. Each block references an S Box and each entry of the S Box outputs a 32 bit data. First, the output of S Box 1 and S Box 2 are added.Then the result of the addition is XORed with SBox 3. Finally, S Box 4 is then added to the output of the XORed operation and provides a 32 bit output.Blowfish is suitable for applications where the key does not change often, like a communications link or an automatic file encrypter. It is significantly faster than most encryption algorithms when implemented on 32 bit microprocessors with large data caches.

4. RSA

RSA(Rivest Shammir Adleman) is public key cryptography algorithm involves two different keys. Public key for encryption and private key for decryption.RSA also provide authentication [7]. RSA Algorithm RSA is a commonly adopted public key cryptography algorithm. RSA can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key.RSA has been widely used for establishing secure communication channels and for authentication and the identity of service provider over insecure communication medium. file. The RSA algorithm involves three steps:

1) 1.Key generation,
2) 2.Encryption and
3) 3.Decryption.

1. Key generation

RSA involves a public key and a private key.The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

Choose two distinct prime numbers p and q. For security purposes, the integer's p and q should be chosen at random. Compute n = p q. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.Choose an integer esuch that $1 < e < \varphi(n)$and gcd(e, φ(n)) = 1; i.e. e and φ(n) are coprime. e is released as the public key exponent.Determine d as $d-1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo φ(n)).This is more clearly stated as solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$d is kept as the private key exponent.By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

2. Encryption

Alice transmits her public key (n, e)to Bob and keeps the private key secret. Bob then wishes to send message M to Alice. He then computes the ciphertext c corresponding to :

$C \equiv m^e \bmod(n)$

Bob then transmits c to Alice.

3. Decryption

Alice can recover m from c by using her private key exponent d via computing:

$m \equiv c^d \pmod{n}$

Given m, she can recover the original message M by reversing the padding scheme.

5. SHA Hash Function

SHA is hash algorithm in which n-bit hash produces a n-bit length finger print from the arbitrary length data[4].SHA-1,SHA-256 ,SHA-512 produces message digest 160,256 and 512 respectively[7]. The Secure Hash Algorithm is a family of cryptographic hash functions published by the National

Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS), including:

- *SHA-0*: The original version of the 160-bit hash function published in 1993 under the name "SHA".
- *SHA-1*: A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm.
- *SHA-2:* A family of two similar hash functions, with different block sizes, known as *SHA-256* and *SHA-512*. They differ in the word size; SHA-256 uses 32-bit words where SHA-512 uses 64-bit words.
- *SHA-3:* It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family.

6. Proposed Work

Our proposed work used the concept of Hash function along with several cryptographic tools to provide better security to the data stored on the cloud. TPA checks the integrity of the data stored on cloud on behalf of the data owner. TPA checks the hash of the message to verify the integrity of the data. The Integrity Verification is provided by the TPA which reduces a lot of work of the data owner. In our proposed system Blowfish and RSA cryptography algorithms are used to integrate the features from both and make it a better system than existing system.

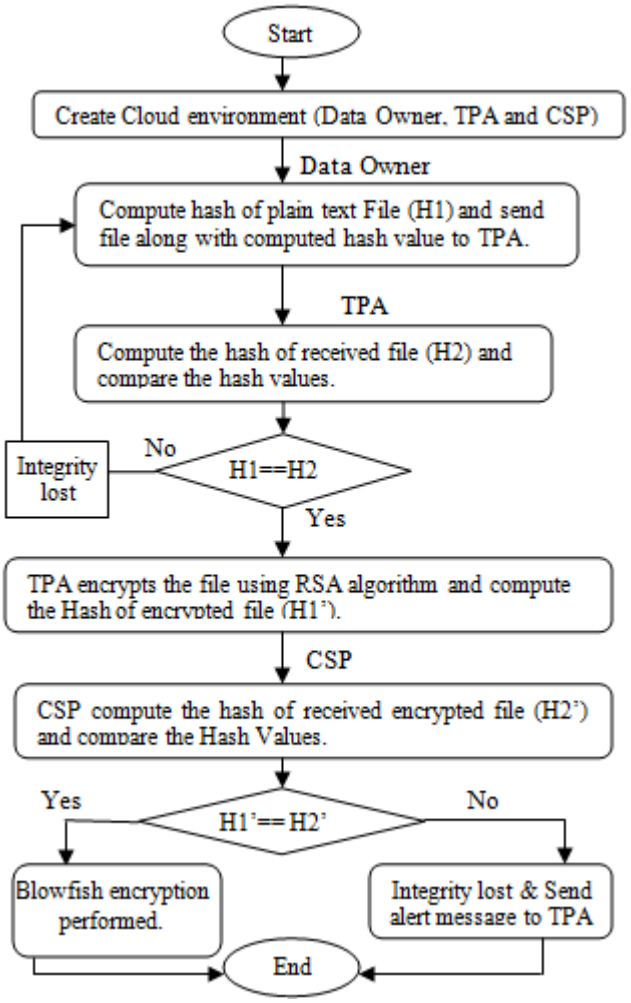

Figure 4: proposed System flow chart

In our proposed work we compare Blowfish, RSA and integrate system (Blowfish+RSA) based on the performance parameters like:- throughput, cipher text, encryption text and delay time. Formulas for these parameters as following :

1) *Throughput:*It is number of bits transferred per unit time . Its unit is byte/sec.
   Formula: Throughput = uploaded file size ÷ Delay time.
2) *Ciphertext size:* It is length of encrypted data. Its unit is in bytes.
   Formula : Ciphertext size = Length of encrypted data
3) *Encryption time:* Time taken by server to encrypt any file. Its unit is nano seconds.
   Formula : Encryption time = Encryption End Time - Encryption Start Time.
4) *Delay Time:* Delay time is time difference between start uploading time and end uploading time. Its unit is in nano seconds.
   Formula : Delay Time = End Uploading Time-Start Uploading Time .

7. Experimental Result

An application has been designed and implemented in java language on the network to achieve the functionalities of the client, TPA and cloud server. We have assumed that the cloud server, TPA and the user are in the same system domain and sharing the uniform system parameters. Based on experiment we have computed the parameters value for RSA , Blowfish and Integrate system(Blowfish+RSA) for a same file. Follwing table shows parameter values for these algorithms:

Table 1: Parameter values

Algorithms → / Factors ↓	RSA	Blowfish	RSA+Blowfish
Encryption Time	239	165	89
Delay Time	7283	7193	7000
Cipher Text	82756	82653	82496
Throughput	20574	20588	20618
File Size	21kb	21kb	21kb

Graph representation corresponding to these factors as following :

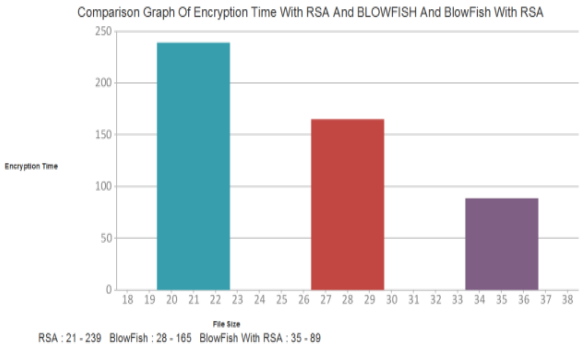

Figure 5: Encryption Time

Graph in fig 5 represents for a file of size 21 kb takes 89 ns encryption time using proposed algorithm (Blowfish+RSA+Hash) which is lesser than Blowfish and RSA encryption time 165 ns and 239 ns respectively.

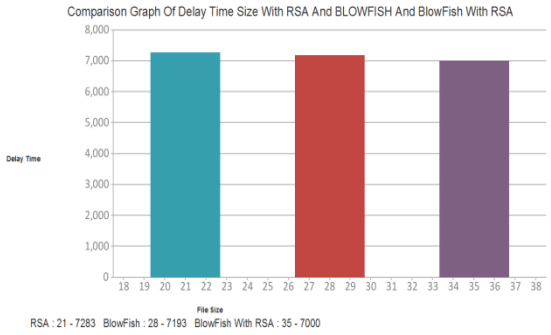

Figure 6: Delay Time

Graph in fig 6 represents for a file of size 21 kb takes 7000 ns delay time using proposed algorithm (Blowfish+RSA+Hash) which is lesser than Blowfish and RSA delay time 7193 ns and 7283 ns respectively.

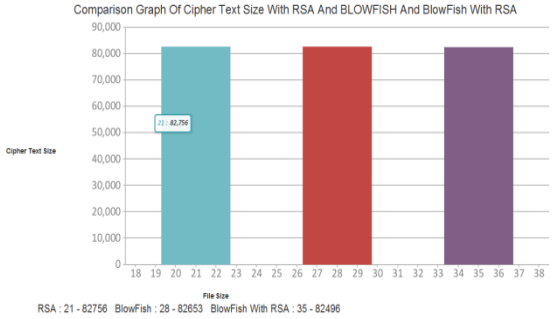

Figure 7: Cipher Text

Graph in fig 7 represents for a file of size 21 kb cipher text size 82496 bytes using proposed algorithm (Blowfish+RSA+Hash) which is lesser than Blowfish and RSA cipher text size 82653 bytes and 82756 bytes respectively.

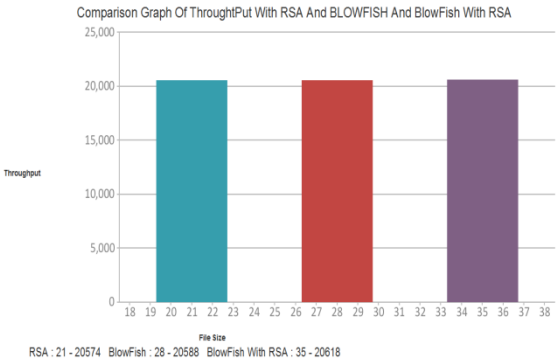

Figure 8: Throughput

Graph in fig 8 represents for a file of size 21 kb throughput is 20618 bytes/sec using proposed algorithm (Blowfish+RSA+Hash) which is more than Blowfish and RSA throughput of 20588 bytes/sec and 20618 bytes/sec respectively.

The criteria in performance of every algorithm is that encryption time ,delay time and cipher text size should be less and throughput should be more. During comparison of RSA, Blowfish and proposed system(Blowfish+RSA+Hash) this criteria is achieved and integrate system of RSA & Blowfish give better results.

8. Conclusion and Future Work

When a client stores its data on the cloud, there is always a big concern of whether the cloud service provider stores the file correctly or not. Security is the main concern in cloud computing. The proposed mechanism provides a security mechanism for securing the data in cloud computing with the help of Blowfish & RSA algorithms and hash function.

This research paper has proposed a system to provide integrity, authentication and confidentiality to the data stored in cloud computing. Authentication is achieved because only registered client upload and download the files on the cloud. The proposed scheme used the combination of blowfish and RSA to secure the data in such a way that no leakage of data on cloud could be performed. Always encrypted file stored on the cloud. Hash value matches at TPA server to check the integrity of file.

There is always a scope for improvement in every field of work, so here also. We take one of the assumption made in all the models of security are that the TPA is neutral. So there is some need to do some work for making TPA more secure. In our proposed system we focus on integrity detection but in future integrity prevention mechanism implemented using some locking techniques.

References

[1] A. Juels and B. S. Kaliski, Jr., (2007) "*Pors: proofs of retrievability for large files,"* in CCS '07: Proceedings of the 14th ACM conference on Computer and Communications security. New York, NY, USA: ACM, 584–597.

[2] Cody, Brian; Madigan, Justin; MacDonald, Spencer; Hsu, Kenneth W.;, "*High speed SOC design for blowfish cryptographic algorithm*," Very Large Scale Integration, 2007. VLSI SoC 2007. IFIP International Conference on , vol., no., pp.284-287, 15-17 Oct. 2007.

[3] Govinda.K1 Mythili and Geetha Priya(2014)," *Data Security in Cloud using Blowfish Algorithm*", International Journal for Scientific Research & Development| Vol. 2, Issue 09.

[4] J. Guo, S. Ling, C. Rechberger, and H. Wang, "*Advanced Meetin-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2*," pp. 1–20.

[5] Gurpreet Kaur and Manish Mahajan (2013), "*Analyzing Data Security for Cloud Computing Using Cryptography Algorithms*", International Journal Of Engineering Research and Application, Vol.-3,782-786.

[6] H. Shacham and B. Waters (Dec.2008), "*Compact Proofs of Retrievability*," In Proceedings. of Asia crypt"08.

[7] Kamak Ebadi,Victor Pena etc."High performance implementation and Evaluation of Blowfish Cryptographic Algorithm on Single-Chip Cloud Computer:A Pipelined Approach ".

[8] K.Govinda, E.Sathiyamoorthy (2012), "*Data Auditing in Cloud Environment using Message Authentication Code*", International Conference on Emerging Trends on Advanced Engineering Research (ICETT).

[9] Ms.Payal P.Kilor and Prof. Vijay B.Gadicha (2014)"*Data Integrity Proofs in Document Management System under Cloud with Multiple Storage*", International Journal of Engineering &Computer Science, vol.3.
[10] Omer K.Jasim et. al.(2013) "*Efficiency of modern encryption algorithms in cloud computing*", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 2.
[11] Paresh D.Sharma, Prof. Hitesh Gupta(February 2014) "*An Implementation for Conserving Privacy based on Encryption Process to Secured Cloud Computing Environment*" IJESRT Sharma, 3(2).
[12] P.Metri and G.Sarote (2013), "*Privacy Issues and Challenges in Cloud Computing*", International Journal of Advanced Engineering Science and Technologies, vol.no.-5,1-6.
[13] R.Buyya, C.S.Yeo, S.Venugopal (2009), "*Cloud Computing and emerging IT platforms: vision, hype and reality for delivering computing"* as 5th utility, Future Generartion Computer System, 25: 599-616.
[14] Schneier, Bruce.(2014) "*Cryptanalysis of MD5 and SHA: Time for a New Standard*". Computerworld. Retrieved .
[15] ShivShakti etc(January-Febuary-2013)."*Encryption using different techniques:A Review*" international journal in Multidisciplinary and academic research (SSIJMAR) vol.2 No.1 (ISSN 2278-5973).
[16] Sravan Kumar and Ashutosh Saxena(2011), "*Data Integrity Proofs in Cloud Storage",* 978-1-4244-8953-4/11/$26.00© IEEE.
[17] S.Subashini and V.Kavitha(2011), "A *Survey on security issues in service delivery models of cloud computing"*. Journal of Network and Computer Applications 34,1-11.
[18] Zaigham Mahmood(2011), "*Data Location and Security Issues in Cloud Computing*", Proceedings of International Conference on Emerging Intelligent Data and Web Technologies