International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 08 | Aug -2017 www.irjet.net p-ISSN: 2395-0072

"A TRUSTED TPA MODEL, TO IMPROVE SECURITY & RELIABILITY FOR CLOUD STORAGE"

Nivedita Roy Gupta[1], Prof. Umesh Kumar Lilhore[2], Prof. Nitin Agrawal[3]

M. Tech. Research Scholar[1], Associate Professor and Head PG[2], Associate Professor[3]
NRI-IIST Bhopal (M.P), India

Abstract- *In now these days Cloud computing is most promising technology for optimum utilization of computing resources. A cloud user can securely store their personal data on cloud storage server and can access anytime. Cloud service providers maintain the reliability and integrity of the stored data over cloud server and ensure cloud user, "Stored data will secure". Day by day the sizes of cloud services are rapidly growing which increases the number of cloud user. Cloud users are demanding more secure communication and storage. A Third party audit (TPA) is used to check the integrity of stored data over the cloud. Cloud data are available over the web, so there are possibilities of attack. So always a secure encryption method is demanding by a cloud user. It attracts cloud researcher to work in the field of cloud security. This research paper presents a trusted TPA model (TTM), to improve the security and reliability for cloud storage. Proposed TTM model is based on two-way security. It provides data security and well as also maintains data integrity. In TTM, AES-256 bit data encryption and decryption methods are used to maintain data security and SHA-1 method is used to calculate the hash values of the message to maintain the data integrity. For a key generation, TTM uses Diffie-Hellmen key exchange method. Proposed TTM and existing AES with MD-5 method both are implemented over JAVA and various performance comparison parameters are calculated such as encryption and decryption time, the time is taken to proceed request and TPA computation time. The experimental study clearly shows that's proposed TTM shows better result over existing MD-5 based method.*

Key Words: **TPA, Cloud Computing, Cloud Security, AES, MD-5, SHA-1, TTMS**

1. INTRODUCTION

Cloud computing has become a big technology trend either within the industrial or the Institute field, and most of the consultants expect that cloud computing can reshape information technology (IT) processes and the IT market place. In cloud computing users connect with the cloud that seems as if it's one entity as critical multiple servers. Cloud computing is referred as two terms, 'Cloud' and 'computing', "Cloud" which used here as a "Metaphor" for the technique are methodology, "the web or the internet", so cloud computing technology is a "type of internet or network based computing". Cloud computing based system can dynamically deliver the computing resources and capabilities as a service over the internet web in all over the world. Cloud computing is a new technique of computing in which dynamically scalable and often virtualized resources are provided as a service over the internet [4]. The wide adaptation of cloud computing is restricted to its aspects of proving security and privacy of the user's data. Data are to be stored remotely at the cloud server where data are to be managed at large data centers. The client can get access to and modify this stored data over the cloud using the network. In cloud computing, a CSP or cloud service providers is a separate administrative entity which available the services to the cloud users.

Data auditing is a new concept introduced in Cloud computing to deal with secure data storage. Auditing is a process of verification of user data. It can be carried out either by the user himself (data owner) or by a TPA. It helps to maintain the integrity of data stored in the cloud. The verifier's role is categorized into two: the first one is private audit ability, in which only user or data owner is allowed to check the integrity of the stored data. No other person has the authority to question the server regarding the data. But it tends to increase verification overhead of the user. Second is public audit ability, which allows TPA to challenge the cloud server and performs data verification checks.

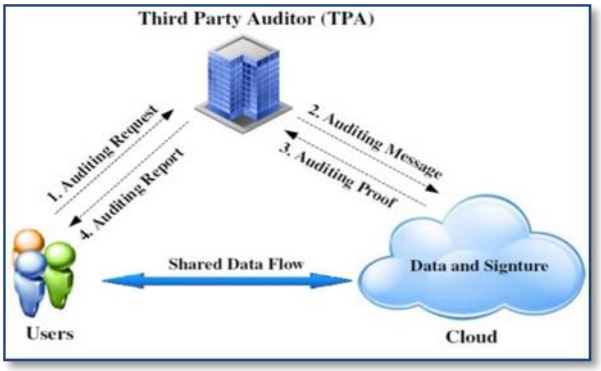

Figure 1.1 TPA Audit in Cloud [8]

The TPA is an entity which is used so that it can act on behalf of the client. It has all the necessary expertise, capabilities, knowledge and professional skills which are required to handle the work of integrity verification. It also reduces the

overhead of the client. It is necessary that TPA should efficiently audit the cloud data. It should have zero knowledge about the data stored in the cloud server. It should not introduce any additional online burden to the cloud data owner [9].In this research paper, a trusted model is proposed for cloud security. This paper is organized in various chapters like cloud computing security, problem statement and objective, proposed solution and result comparisons.

2. CLOUD COMPUTING & SECURITY THREATS

"Cloud computing technology is a large scale based distributed computing and vitalization based technology that is widely used by and driven by various economies of scale. In cloud computing, a large pool of servers and computing resources directly serves to various users on demand, based on pay per and use, over the network such as web or internet. Cloud computing provides service such as abstraction of data, virtualization, dynamically scalable computing power, platform, and storage". According to Armbrust (the year 2009), "Cloud Computing technique basically refers to all the applications which are delivered as services directly over the Internet network and the systems software and hardware applications in the cloud data centers that serve these cloud computing services, referred to as Software as a Service (SaaS). As per NIST cloud computing can be defined-"Cloud computing is a model for enabling ubiquitous, 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 service provider interaction"

2.1 Major threats in cloud computing-

Major issues in cloud computing are as follows-

- **Data breaches** - As enterprises stores vast data in the cloud, it becomes an attractive target for the hackers. In a case of security breaches involving financial data, healthcare data, and revenue details can be more devastating. It may lead an enterprise to incur fines, face lawsuits or even criminal charges.

- **Compromising Credentials** - A well-defined Identity and Authentication technology where enterprises provide to right access to the right person at the right time. Sometimes they fail to remove user access even after they left the organizations which could lead to obtaining their credentials.

- **Hacking Application Programming Interface**- To interacts with the cloud services enterprise uses interfaces and API. The overall cloud security (Authentication, access control, monitoring depends highly on the security of the API).

- **Exploiting system vulnerabilities-**The multi-tenancy in cloud computing where enterprises share memory, databases and other digital resources may create new attack surfaces. This can become bigger security issues if hackers could exploit system vulnerabilities or bugs.

- **Hijacking the accounts-**In Cloud, Computing attackers can eavesdrop on financial transaction activities change or could modify it. Multifactor authentication can be a common defense-in-depth protection strategy.

- **Malicious insiders-**In cloud computing insider threat can shatter the complete infrastructure and data manipulation. Therefore enterprises should control the encryption process and minimize the user access.

- **Advanced Persistent threats-**APTS are the parasitical form of attacks and are difficult to detect. Enterprises should monitor the costs involved to overcome APT attacks improper planning would increase the enterprise's security spending.

- **Data Loss**-When an authorized user uploads files to the cloud there are chances for data loss that can be extremely costly for an enterprise. A recent report from the Health Information Trust Alliance (HITRUST) total number of breaches in the healthcare industry "Total cost of breach - $4.1 billion" Therefore enterprises should deploy a Data Loss Prevention (DLP) system plan.

- **DDoS attacks-**In cloud environment enterprises should be aware of application-level Dos attacks targeting web server and database vulnerabilities.

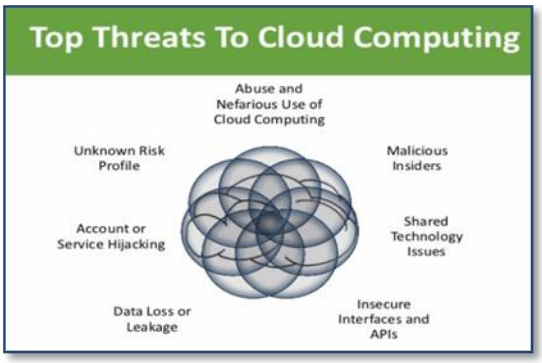

Figure 2.1 Cloud security risks [5]

2.2 HASH Vs MAC BASED INTEGRITY

A cryptographic hash function is a completely public, deterministic hash function which everybody can compute over arbitrary inputs. It takes as input a sequence of bits (any sequence of bits; some hash functions are formally limited to inputs of, say, less 264 bits, aka "2 millions of terabytes") and outputs values in a rather small space, typically a sequence of bits with a fixed size (e.g. always 160 bits with the standard hash function SHA-1). Good cryptographic hash functions respect some conditions which boil down to, informally, that they mix input data so thoroughly that we cannot figure it out afterward.

A message authentication code is an algorithm which takes as input a message and a secret key and produces a fixed-size output which can be later on verified to match the message; the verification also requires the same secret key. Contrary to hash functions where everything is known and attackers are fighting against mathematics, MAC makes sense in models where there are entities with knowledge of a secret. What we expect from a good MAC is unforgeability: it should be infeasible to compute a pair message +MAC value which successfully verifies with a given key K without knowing K exactly and in its entirety.

Hash functions and MAC are thus distinct kind of algorithms with distinct properties and used in really distinct situations. Some MAC algorithms (but certainly not all of them) can be thought of as "hash functions with a key" but this is a restrictive view. HMAC is a well-known MAC construction, which itself builds on an underlying hash function in a smart way. Indeed, security properties and models for hash functions and MAC are sufficiently distinct from each other that slapping a hash function and a key together does not necessarily yield a secure MAC, even if the hash function is secure (see the length extension attack which illustrates that point).

3. PROBLEM STATEMENT AND OBJECTIVE

Cloud service providers maintain the reliability and integrity of the stored data over cloud server and ensure cloud user, “Stored data will secure”. Day by day the sizes of cloud services are rapidly growing which increases the number of cloud user. Cloud users are demanding more secure communication and storage. A Third party audit (TPA) is used to check the integrity of stored data over the cloud. Cloud data are available over the web, so there are possibilities of attack. So always a secure encryption method is demanding by a cloud user. It attracts cloud researcher to work in the field of cloud security. Existing methods encounters with several issues such as-

- Encryption and decryption time
- TPA Computation time
- Storage Cost
- Avalanche Effect
- Privacy & Integrity

This research paper presents a trusted TPA model (TTM), to improve the security and reliability for cloud storage. Proposed TTM model is based on two-way security. It provides data security and well as also maintains data integrity. In TTM, AES-256 bit data encryption and decryption methods are used to maintain data security and SHA-1 method is used to calculate the hash values of the message to maintain the data integrity. Proposed TTM method will be achieved-

- Efficient encryption and decryption
- Better computation time
- Optimum storage cost
- Better avalanche effect
- Better Privacy & Integrity

4. PROPOSED TRUSTED MODEL

Cloud users are demanding more secure communication and storage. A Third party audit (TPA) is used to check the integrity of stored data over the cloud. Cloud data are available over the web, so there are possibilities of attack. So always a secure encryption method is demanding by a cloud user. It attracts cloud researcher to work in the field of cloud security. This research paper presents a trusted TPA model (TTM), to improve the security and reliability for cloud storage. Proposed TTM model is based on two-way security. It provides data security and well as also maintains data integrity. In TTM, AES-256 bit data encryption and decryption methods are used to maintain data security and SHA-1 method is used to calculate the hash values of the message to maintain the data integrity.

4.1 Working with Proposed TTM Model-

The system provides a hash, access list, encryption/decryption by a trusted third party over the network in the form of "Software as a Service" (SaaS). The trusted 3rd party which provides these security services does not store any data at its ends, and stores the only master key for each client for data encryption and decryption, and a hash of the data which is calculated on the client side. To enhance the security, the communication between client and security server is secured using the Diffie-Hellmen key, which is used as an input for AES. This division of responsibility has a big effect, as no single provider has access to other data and security key, a hash at the same time. Proposed TTM has following modules-

- Data Upload Module
- Key generation and key exchange (Diffie-Hellman) module

- Encryption (AES-256)& Hash Generation (SHA-1)Module
- TPA Verification Module

4.2 Proposed TTM Algorithm-

TTM Algorithm for Cloud privacy and data integrity-
Key Generation Module-
Steps in the algorithm:
Step-1 Sender and Receiver agree on a prime number p and a base g.
Step-2 Sender chooses a secret number a, and sends Receiver (g^a mod p).
Step-3 Receiver chooses a secret number b and sends Sender (g^b mod p).
Step-4 Sender computes ((g^b mod p)^a mod p)
Step-5 Receiver computes ((g^a mod p)^b mod p)
Both Sender and Receiver can use this number as their key. Notice that p and g need not be protected.

AES-256 Encryption Module-
Step-1 Key Expansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
Step-2 initial round
2.1 AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
Step-3 Rounds
3.1 SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
3.2 ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
3.3 MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
3. 4 AddRoundKey
Step-4 Final Round (no MixColumns)
4.1 SubBytes
4.2 ShiftRows
4.3 AddRoundKey.
SHA-1 (Hash Generation Module)
Step 1: Append Padding Bits….
The message is "padded" with a 1 and as many 0's as necessary to bring the message length to 64 bits less than an even multiple of 512.
Step 2: Append Length....
64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.
Step 3: Prepare Processing Functions….
SHA1 requires 80 processing functions defined as:
f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)
f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)
f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)
f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)
Step 4: Prepare Processing Constants....
SHA1 requires 80 processing constant words defined as:
K(t) = 0x5A827999 (0 <= t <= 19)
K(t) = 0x6ED9EBA1 (20 <= t <= 39)
K(t) = 0x8F1BBCDC (40 <= t <= 59)
K(t) = 0xCA62C1D6 (60 <= t <= 79)
Step 5: Initialize Buffers….
SHA1 requires 160 bits or 5 buffers of words (32 bits):
H0 = 0x67452301
H1 = 0xEFCDAB89
H2 = 0x98BADCFE
H3 = 0x10325476
H4 = 0xC3D2E1F0
Step 6: Processing Message in 512-bit blocks (L blocks in total message)….
This is the main task of an SHA1 algorithm which loops through the padded and appended message in 512-bit blocks.
Input and predefined functions:
M[1, 2, ..., L]: Blocks of the padded and appended message
f(0;B,C,D), f(1,B,C,D), ..., f(79,B,C,D): 80 Processing Functions
K(0), K(1), ..., K(79): 80 Processing Constant Words
H0, H1, H2, H3, H4, H5: 5 Word buffers with initial values
Step 6: Pseudo Code….
For loop on k = 1 to L
(W(0),W(1),...,W(15)) = M[k] / Divide M[k] into 16 words */*
For t = 16 to 79 do:
W(t) = (W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)) <<< 1
A = H0, B = H1, C = H2, D = H3, E = H4
For t = 0 to 79 do:
TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t) E = D, D = C, C = B<<<30, B = A, A = TEMP
End of for loop
H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E
End of for loop
Output: H0, H1, H2, H3, H4, H5: Word buffers with final message digest

5. IMPLEMENTATION AND RESULT ANALYSIS

In cloud computing security plays a vital role in cloud performance. Auditing protocols and privacy preserving system helps cloud user and cloud service providers to maintain cloud security and trust. Efficient auditing systems are always desirable for the cloud. Cryptography methods are used to encrypt and decrypt stored data over cloud server.

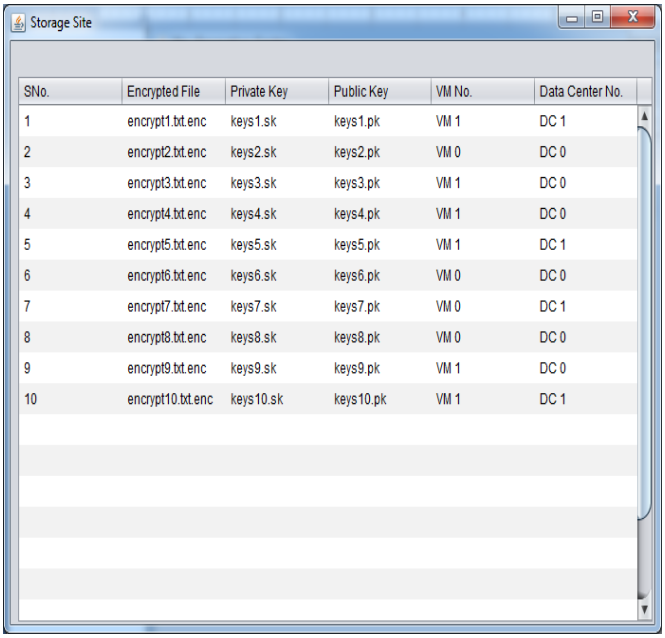

Figure 5 Implementation Screenshot for TTM Model

Proposed TTM (SHA-1+ AES) and existing Method (AES+ MD-5) both are implanted over Cloud Sim-3.1 simulator with JAVA Net Beans. Following results were calculated-

5.1 Encryption and Decryption time-

Total time which requires encrypting a plain text message into its equivalent cipher text is called encryption time and time that requires to converts a cipher text message into its equivalent plain text are called decrypt a cipher text. Less encryption and decryption time for a method shows better performance.

File Size in MB	Encryption Time in ms			
	Existing method		Proposed method TTM	
	Encryption	Hashing	Encryption	Hashing
20	16945	14788	15478	13898
15	13502	9045	12778	8257
10	12789	8789	10789	7504
5	9898	6898	8729	5898

Table 5.1.1 Encryption Time

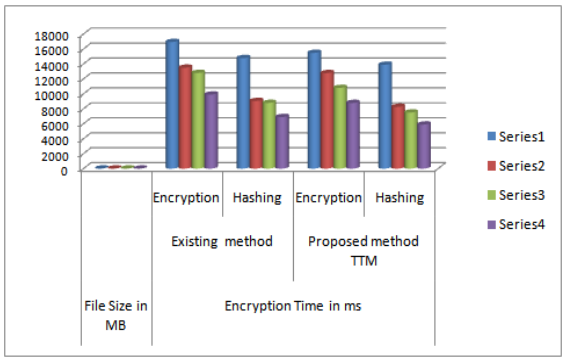

Figure 5.1.1 Graph Encryption Time

File Size in MB	Decryption Time in ms			
	Existing method		Proposed method TTM	
	Decryption	Hashing	Decryption	Hashing
5	8598	7898	7589	6989
10	7895	5898	5145	4789
15	6585	5245	4102	3245
20	5669	4855	3989	2145

Table 5.1.2 Decryption Time

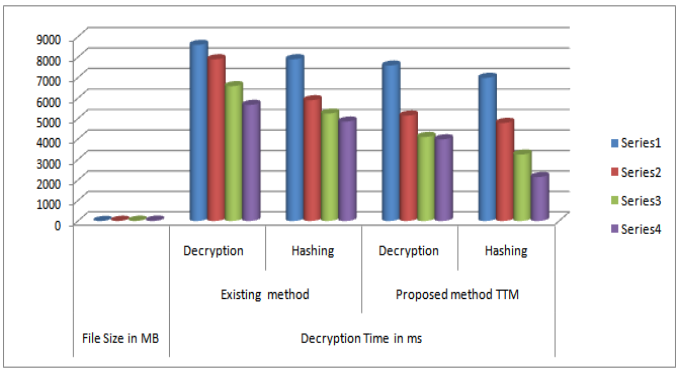

Figure 5.1.2 Graph Decryption Time

Influences- The above table and graph 5.1.1 & 5.1.2 clearly shows that proposed **TTM (SHA-1+ AES)** shows better encryption and decryption time as compared to existing Method **(AES+ MD-5).**

5.2 TPA Computational Time-

Total time consumed during the auditing process. It is the amount of time for which a server was used for processing a file which is stored on a cloud server. Less TPA computational times for auditing of a file or data shows better performance of the cloud system.

File Size in MB	TPA Computational Time in ms	
	Existing method	Proposed method TTM
	Encryption	Encryption
5	18989	16745
10	20489	17895
15	22989	18985
20	25028	19256

Table 5.2.1 TPA Computational Time

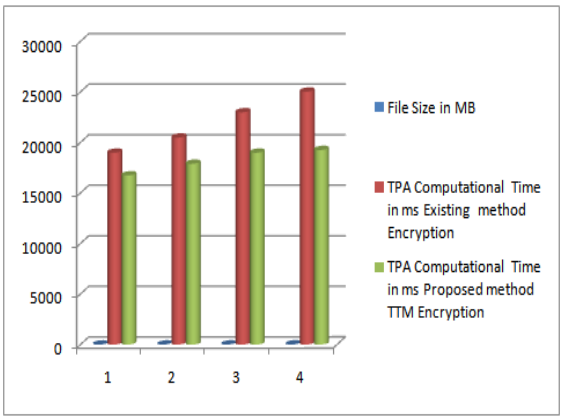

Figure 5.2.1 Graph TPA Computational Time

Influences- The above table and graph 5.2.1 clearly shows that proposed **TTM (SHA-1+ AES)** shows better TPA Computational time as compared to **existing Method (AES+ MD-5).**

5.3 Avalanche Effect %-

In cryptography, the avalanche effect refers to an attractive property of block ciphers and cryptographic hash functions algorithms. The avalanche effect is satisfied if: The output changes significantly (e.g., half the output bits flip) as a result of a slight change in input (e.g., flipping a single bit).

No of bit changes in	Avalanche Effect %	
	Existing method	Proposed method TTM
1	84.25	88.1
2	88.45	91.25
3	90.25	92.33

Table 5.3.1 Avalanche Effect %

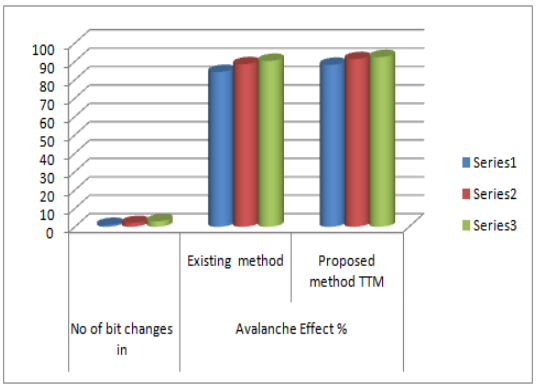

Figure 5.3.1 Graph Avalanche Effect %

Influences- The above table and graph 5.3.1 clearly shows that proposed **TTM (SHA-1+ AES)** shows better Avalanche effect as compared to **existing Method (AES+ MD-5).**

6. CONCLUSIONS & FUTURE WORK

Cloud computing has different security issues in threats in user view, one can say that lack of security is the only worth mentioning disadvantage of cloud computing. The bond between service providers and users is necessary for providing better cloud security. This paper presented a TPA based privacy preserving and security model for cloud computing. Proposed TTM model is based on two-way security. It provides data security and well as also maintains data integrity. In TTM, AES-256 bit data encryption and decryption methods are used to maintain data security and SHA-1 method is used to calculate the hash values of the message to maintain the data integrity. For a key generation, TTM uses Diffie-Hellmen key exchange method. The experimental study clearly shows that proposed method performs outstandingly in terms of encryption and decryption time, computation time, avalanche effect over existing (AES+MD-5) method. In future work, we can implement proposed method with the more realistic scenario and data, with new standards. And can compare with more security methods.

REFERENCES

[1]. *Swapnali S. More, Sangita S. Chaudhari," Secure and Efficient Public Auditing scheme for Cloud Storage", 2016 International Conference on Computing, Analytics and Security Trends (CAST), IEEE College of Engineering Pune, India. Dec 19-21, 2016, PP 439-445.*

[2]. *Bhale Pradeep kumar Gajendra, Vinay Kumar Singh, More Sujeet," Achieving Cloud Security using Third Party Auditor, MD5 and Identity-Based Encryption", International Conference on Computing, Communication and Automation (ICCCA2016) IEEE, 2016, PP1304-1310.*

[3]. *Rajat Saxena and Somnath Dey, "Cloud Audit: A Data Integrity Verification Approach for Cloud Computing, Twelfth International Multi-Conference on*

Information Processing-2016 (IMCIP-2016), Science Direct 2016, PP 142-152

[4]. *Swapnali More, Sangita Chaudhari,"Third Party Public Auditing scheme for Cloud Storage", 7th International Conference on Communication, Computing and Virtualization 2016, Science Direct, PP 69-77*

[5]. *Shruti Batham, Umesh Lilhore and Sini Shibu "Improved HLA based encryption process using fixed size aggregate key generation", Journal of Modern Trends in Engineering and Research, vol. 2, issue 1, Jan 2015.*

[6]. *Ankita R. Makode, V. B. Bhagat," Privacy Preserving For Secure Cloud Storage", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume, 4 Issue, 4, PP 475-479*

[7]. *Shruti Batham, Umesh Lilhore, Sini Shibu.,"Improve HLA based Encryption Process using fixed Size Aggregate Key generation", IJMTER, International Journal of Modern Trends in Engineering and Research Volume 2, Issue 1, (01 - 2015), PP 239-245.*

[8]. *F. Sebhe, J. Domingo-Ferrer, A. Martinez-Ballast, Y. Deswarte and J.-J. Quisquater,"Efficient Remote Data Possession Checking in Critical Information Infrastructures", IEEE Trans. Knowl. Data Eng., vol. 20(8), pp. 1034–1038, (2008).*

[9]. *C. C. Erway, A. Kupcu, C. Papamanthou and R. Tamassia,"Dynamic Provable Data Possession", ACM Conference on Computer and Communications Security, pp. 213–222, (2009).*

[10]. *L. Chen, Using Algebraic Signatures to Check Data Possession in Cloud Storage, Future Generation Comp. Syst., vol. 29 (7) pp. 1709–1715, (2013).*

[11]. *A. Jules and B. S. K. Jr., "Pors: Proofs of Retrievability for Large Files", In ACM Conference on Computer and Communications Security, pp. 584–597, (2007).*

[12]. *H. Shacham and B. Waters, "Compact Proofs of Retrievability", IACR Cryptology print Archive 2008, vol. 73, (2008).*

[13]. *K. D. Bowers, A. Juels and A. Opera," Proofs of Retrievability: Theory and Implementation", In Proceedings of the 2009 ACM Workshop on Cloud Computing security, ACM, pp. 43–54, (2009).*

[14]. *A. Jules, K. D. Bowers and A. Oprea, "Hail: A High-Availability and Integrity Layer for Cloud Storage", In ACM Conference on Computer and Communications Security, pp. 187–198, (2009).*

[15]. *C. Wang, Q. Wang, K. Ren and W. Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, In INFOCOM, pp. 525–533, (2010).*

[16]. *Q. Wang, C. Wang, J. Li, K. Ren and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", In Computer Security–ESORICS 2009, Springer, pp. 355–370, (2009).*

[17]. *Akkala. Sai babu, T. Satyanarayana Murthy "Security provision in the publicly auditable secure cloud data storage of computer services using sha-1 algorithm" et al, International journal of computer science and information technologies Vol.3 (3), 2012.*

[18]. *Kuyoro S. O., Ibikunle F., Awodele O.," Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3): Issue (5): 2011, PP 247-255.*

[19]. *W. Jansen, T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", December 2011, NIST Special Publication 800-144.*

[20]. *S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained access control in cloud computing," in Proc. of IEEE INFOCOM'10, San Diego, CA, USA, March 2010.*

[21]. *W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188, 2009.*