A Survey On Data Security and Storage Mechanism In Cloud Computing

Digant. N. Parmar[1], Kalpesh L. Patel[2]

[1]*Student, Computer Engineering Department, L.C. Institute of Technology, Gujarat, India*
[2] *Assistant Professor, Computer Engineering Department, L.C. Institute of Technology, Gujarat, India*

ABSTRACT

Cloud computing, often referred to as simply "the cloud", is the delivery of on-demand computing resources - everything from applications to data centers-over the internet on a pay-for-use basis. The cloud storage contributors are in charge for monitoring the data which is available and accessible on the cloud. It is a dreadfully challenging part to maintain the security of data stored in third party cloud database. The stored data in cloud is so important that the user ensures that no data is corrupted or lost. Much research work has been done on data security using RSA with a traditional approach and logic. The entitled research work emphasize on a robust scheme to provide integrity, privacy, and confidentiality to data stored on the cloud .The scheme emphasize on security and authentication using efficient RSA with key encryption MD5 along with the efficient mechanism for data being stored in the data centers . RSA algorithm uses efficient two public key pairs rather than sending the encryption value directly as a public key. Work is done on load balancing technique and on other performance parameters like load capacity, PSNR, time and security.

***Keywords* :-** *Cloud computing, Data security, RSA,MD5.*

---

1. INTRODUCTION:

Most importantly the cloud environment deteriorates the perception of perimeter security. Perimeter security is a set of physical and programmatic security policies that provide levels of protection on a conceptual borderline against remote malicious activity. Traditionally, it is believed that any connectivity to systems or organizations outside of an organization provide an opening for unauthorized entities (personnel or processes) to gain access or tamper with information resources. Upon this static conceptual boundary, security controls were deployed to protect the Information System within it. In a cloud computing model, the perimeter becomes fuzzy, weakening the effectiveness of this measure. The emergence of cloud service models, is expected to lead to a deconstruction of the application services as they are already delivered in existing ''closed'' service provisioning environments. [11]

"Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing." [15]
Cloud computing due to its architectural design and characteristics imposes a number of security benefits, which include centralization of security, data and process segmentation, redundancy and high availability. While many traditional risks are countered effectively, due to the infrastructures singular characteristics, a number of distinctive security challenges are introduced. Cloud computing has ''unique attributes that require risk assessment in areas such as availability and reliability issues, data integrity, recovery, and privacy and auditing''.[16]

1.2 Data Security:

As cloud computing is achieving increased popularity, concerns are being expressed regarding the security issues introduced through acceptance of this new form. The usefulness and efficiency of conventional defense mechanisms are being reconsidered as the features of this new deployment model can differ widely from those of traditional architectures. The other outlook on the topic of cloud security is that this is but another, although fairly expensive, a

case of "applied security" and that alike security ethics that apply in collective multi-user mainframe security models apply with cloud security. The relative security of cloud computing services is a contentious issue that may be delaying its acceptance. Physical control of the Private Cloud equipment is more secure than having the equipment off site and under someone else's control. Physical control and the ability to visually examine data links and access ports is required in order to make certain that the data links are not compromised. Issues barring the adoption of cloud computing are due in large part to the private and public sectors' unease surrounding the external management of security-based services. It is the very nature o fcloud computing-based services, private or public, that promote external management of provided services. This delivers the great incentive to cloud computing service providers to prioritize building and maintaining strong management of secure services. Security issues have been categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. Solutions to various cloud security issues vary, from cryptography, particularly public key infrastructure (PKI), to use of multiple cloud providers, standardization of APIs, and improving virtual machine support and legal support**.** [12]

1.3 Data Confidentiality:

Data confidentiality is one of the major issues, when outsourcing highly sensitive data to the cloud. Data confidentiality makes sense that the confidential data must be inaccessible to the unintended users. Data confidentiality can be ensured by strict access control policies. There must be a policy such that the unintended users must not infer anything from the information being stored in the cloud database. [6]

1.4 Data Integrity:

Data integrity is the most important facet of security in cloud computing. Data integrity aims to safeguard data from alteration or deletion by illegitimate users. Data integrity can be effortlessly accomplished in centralized systems. However, it is a complex task to be achieved in distributed cloud computing environment .Most of the adversaries aim to delete or modify the cloud data, which is a very serious issue.[6] Data Integrity refers to protecting data from unauthorized deletion, modification or fabrication. Managing an entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated or stolen. By preventing unauthorized access, organizations can achieve greater confidence in data and system integrity. Additionally, such mechanisms offer the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity (accountability).[11]

1.5 Availability:

Availability refers to the property of a system being accessible and usable upon demand by an authorized entity. System availability includes a systems ability to carry on operations even when some authorities misbehave. The system must have the ability to continue operations even in the possibility of a security breach. Availability refers to data, software but also hardware being available to authorized users upon demand. Leveraging users from hardware infrastructure demands generates a heavy reliance on the ubiquitous network's availability. [11]

1.6 Data Locality:

The consumers are unaware that, where there data is being resided. In some cases it is an issue for some companies for data privacy laws in various countries. So, the service model must be capable of proving data security based on location issues.

1.7 Access Control:

Solutions to maintain privacy in cloud computing include strategy and legislation as well as end users' choices for how data is stored. The cloud service provider should establish obvious, clear and related policies that explain how the data of each cloud consumer will be accessed and used. The users can change the form of the data that is processed or stored within the cloud to prevent unofficial access. The best options are Cryptographic encryption mechanisms. In addition authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit. Strong authentication is an obligatory requirement for any cloud deployment. User verification is the chief basis for access control, and mainly in the cloud environment, authentication and access control is more important than ever since the cloud and all of its data are publicly accessible. Cloud ID delivers privacy saving cloud based and cross-enterprise biometric recognition solutions for this issue. It relates the private data of the customers to their biometrics and preserves it in a changed form to hide its meaning. Using the searchable encryption procedure. Identification of the user is done in the encrypted field to make

sure that the cloud giver or possible attacker cannot access any confidential data or even the information of the queries on a user.[12]

1.8 Cloud Storage

Using the cloud storage, data is stored on numerous third party servers, formerly on the steadfast server's uses in antiquated network data storing. When store data, the operator perceives an imitation server that is to say, it seems as if the data is storing in a specific location with particular designation. Conversely, that location does not be existent in actuality. It is just a penname familiar mention virtual space engraved out of the cloud computing. The operator's data could be stored on any more than of computers used to produce the cloud computing.[9]

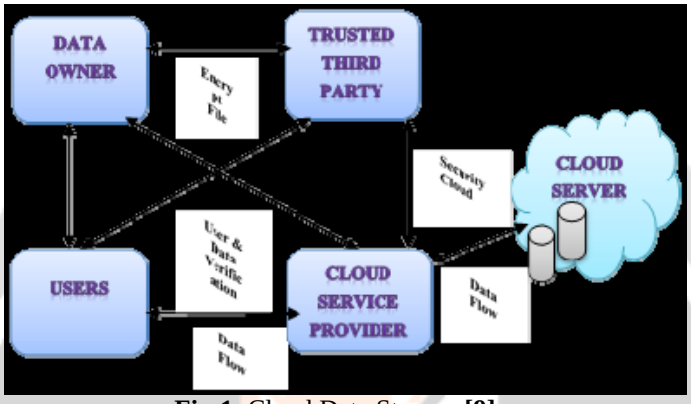

Fig-1: Cloud Data Storage **[9]**

2. LITERATURE REVIEW:

2.1"Enhancing data storage security in Cloud using Certificate less public auditing" [1]

Authors have proposed a scheme namely certificate less public auditing scheme to enhance the data storage security. The main component of the proposed system is TPA (Third Party Auditor), KGC (Key generation centre), user and the Cloud server. Rather than using certificates the authors have proposed a scheme based on the public key and private key mechanism. The end user asks for a audit to TPA and at the same time it provides its identity to KGC and obtains a partial private key. Public and private key is generated based on the partial private key provided by KGC. The TPA would raise a challenge to the cloud server and the cloud server will provide a proof. After authenticating the proof the auditing result is sent to the user.

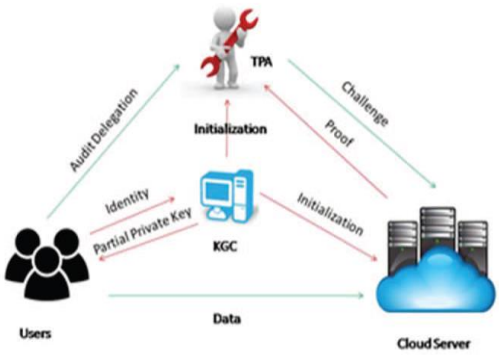

Fig-2: Certificate less Public Auditing[1]

Algorithms being used are Merkel hash tree algorithm(Ralph Merkel -1979) and billinear mapping .working of merkel algorithm is shown in figure below.

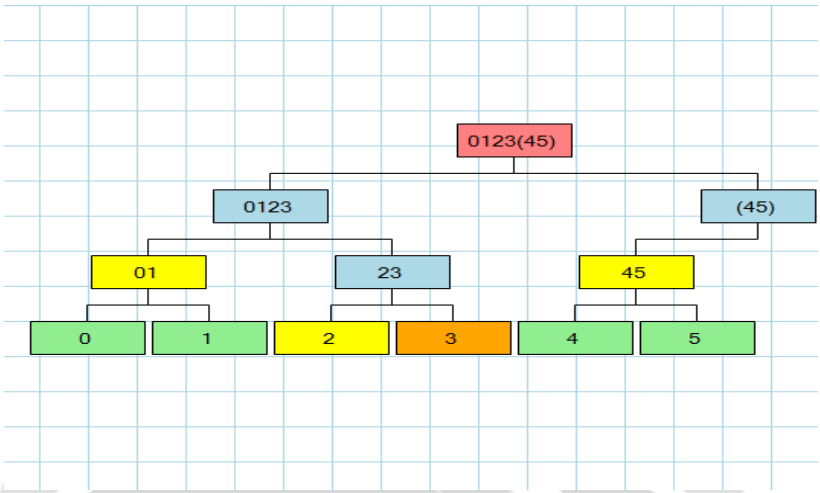

Fig-3: Merkel hash tree algorithm [13]

Future scope:

The existing work does not provide data integrity. The generation of keys and their management is an issue. So work can be done so as to provide data integrity and proper key management mechanism. The efficiency of proposed system can be mapped by using other algorithms.

2.2 "Data security in cloud computing and outsourced databases" [2]

Authors introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication.

The main method being used is homomorphic encryption. The method proposed here provides a cheating detection mechanism to verify computational results from previous algorithm iterations. Matrix vector multiplication is used to design a batch result verification mechanism.

Future scope:

Since the iterative method is used here the work can be done to improve the speed. The major drawback of this method is that it relies on the previous algorithm iterations .Work can also be done on lager data sets.

2.3 "Enhancing data and privacy security in mobile cloud through quantum cryptography"[3]

(QKD) BB84 Quantum Key Distribution protocol
TNRN (Trusted NFC Relay Node)
DWDM (Dense Wavelength Division Multiplexing)

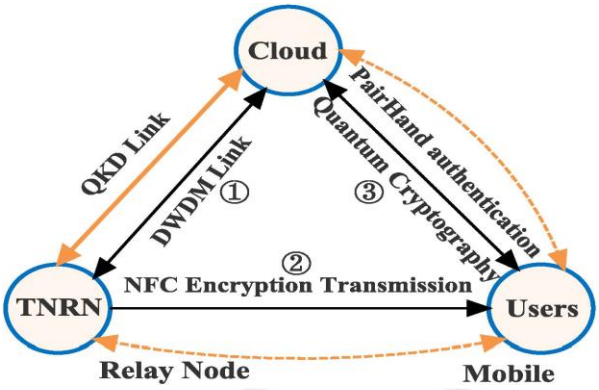

Fig-4: Quantum cryptography security model in mobile cloud [3]

Basis	**0**	**1**
+	↑	→
×	↗	↘

Table-1: Quantum basis [14]

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
Shared secret key	0		1			0		1

Table-2: Quantum key cryptography [14]

Authors have proposed a security model for mobile cloud computing based on quantum cryptography. BB84 Quantum Key Distribution protocol and Near Field Communication (NFC) technology has been used. The working and key generation process is shown in the figure and table above.

Future Scope:

The method proposed here provides QCMC(Quantum Cryptography Security Model In Mobile Cloud Computing) model for data security. But still there are vulnerabilities like noise mixing, rely attack, eavesdropping, etc .So work can be done to prevent the system from such vulnerabilities.

2.4"A comprehensive evaluation of cryptographic algorithms in cloud computing," [4]
Authors have used three different algorithms namely AES(Advance Encryption Standard), RSA and MD5(Message Digest 5) and mapped them. The experimental evaluation is done on different input sizes: 2kb,5kb,20kb,and 50kb. They found that AES and MD5 uses the least time and memory usage is also low.

Future Scope:
In future work can be done to improve the scalability and performance of RSA algorithm and MD5 on a larger block of data and results can be mapped.

2.5 "Efficient privacy preserving integrity checking model for cloud data storage security" [5]
Authors have proposed a scheme that is able to detect the corrupted data by an active adversary. Their auditing protocol uses digital signature algorithm in association with certificates. The proposed scheme is very much effective in privacy preserving.

Future Scope:
The uniqueness of the random signature value are critical in the proposed system. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping signature value secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to reveal the private key .So work can be done to prevent the private key and digital signature value.

2.6 "A short review on data security and privacy issues in cloud computing" [6]
Authors have presented a review and literature analysis of various papers about the data security. Authors have focused on issues like data confidentiality, data integrity, data availability and data privacy. Methods like provable data possession, third party auditing and public auditing have been used to provide data security.
While using the above mentioned methods to provide data security various issues are found. To provide data integrity PDP and auditing schemes are used that lifts the issues like time complexity, data management, computational complexity and trust. To provide data confidentiality methods being used are encryption ,layer based security and concealment of data. This give rise to issues like key count cost, time and computational complexity and large size data.

Future Scope:
The work can be done to improve various performance parameters like time and computational complexity. An efficient mechanism may be developed to provide security of voluminous data and work can be done on key management and data management.

2.7"Ensuring data storage security in cloud computing based on hybrid encryption schemes," [7]
Authors have proposed a hybrid encryption scheme to secure the data at rest. This scheme provides a mechanism of securing the stored data. No specific methods are discussed by the authors to secure the data during data transfer. A algebraic summation method is used for key generation. An attacker can easily break the system if small prime numbers are used and it becomes slow and complex if large prime numbers are used.

Future Scope:
Work can be done and results can be mapped to secure the data during transfer using the same mechanism .Since the system is based on shared secret key mechanism there are chances of keys being stolen or malfunctioned. Moreover it does not focus on error localization.

2.8"Scheme for ensuring data security on cloud data storage in a semi-trusted third party auditor," [8]
The authors have used ECC and AES algorithms to secure data and prevent leakage in the cloud.AES encryption is used during auditing so that the third party auditor will not be able to get the original content of data.ECC encryption is used during the transmission of data and it prevents the attack like Man In The Middle (MITM)attack. The proposed scheme consists of four algorithms, namely, KeyGen, MetaGen, SigGen and Verify Proof. KeyGen is run

by the client and the third party auditor (TPA) to configure the scheme. Client uses MetaGen to generate metadata using SHA-256 during auditing so as to ensure data integrity. SigGen is used by the client to generate signature or tag for authentication.VerifyProof is used to generate a proof of data storage correctness by the TPA top verify the received file from the cloud server.

Future Scope:
Work can be done on biclique attacks which are a variant of meet in the middle attack. In the mathematical field of graph theory, a complete bipartite graph or biclique is a special kind of bipartite graph where every vertex of the first set is connected to every vertex of the second set. The intermediate values for the plain- and cipher text cannot be computed independently in the MITM attack. The more rounds you attack, the larger sub ciphers you will have. So you will have to brute force fewer independent key-bits between the sub ciphers independently. For instance allow one to seven round of AES 128 using MITM attacks, and then by utilizing a biclique structure of length 3 (i.e. it covers 3 rounds of the cipher), you can map the intermediate state at the start of round 7 to the end of the last round.

3. COMPARATIVE TABLE:

Table-3 Table Of Comparison

SR. NO	TITLE	METHOD/ALGORITHM	DRAWBACK AND FUTURE SCOPE
1	Enhancing Data Storage Security In Cloud Using Certificate less Public Auditing	Certificate less Public Auditing Scheme. Merkle Hash Tree Algorithm	Key management problems can occur. Work can be done on key management.
2	Data Security in Cloud computing and Outsourced Databases	Cheating detection mechanism Homomorphic Encryption	Iterative method is applied on block level data. Work can be done on large size data.
3	Enhancing Data and Privacy Security in Mobile Cloud Computing through Quantum Cryptography	Quantum cryptography Quantum cryptography security model(QCSM) QuantumKey Distribution Protocol	Work can be done to prevent relay attack and eavesdropping.
4	A Comprehensive Evaluation of Cryptographic Algorithms in Cloud Computing	RSA AES MD5	Speed, Scalability, Authentication, Memory usage and Power Consumption can be improved.
5	Efficient Privacy Preserving Integrity Checking Model for Cloud Data Storage Security	Digital Signature Algorithm and Certificates	Eucalyptus tool is used. Other tools can be used to achieve more efficient results.
6	A Short Review on Data Security and Privacy Issues in Cloud Computing	Lightweight security mechanism by data encryption.	Key count cost can be reduced
		Encrypted data Searching	Time complexity is an issue.
		Security as a service	Computational Complexity is more.

		Concealment Of Data	Voluminous Data concealment is complex.
7	Ensuring Data Storage Security In Cloud Computing Based On Hybrid Encryption Schemes	Hybrid encryption and decryption schemes are used.	Error localization and communication delay needs to be addressed.
8	Scheme for Ensuring Data Security on Cloud Data Storage in a Semi-trusted Third Party Auditor	ECC encryption function is used to provide Confidentiality. AES algorithm is used to secure data.	Data integrity to third party auditor
9	Data Security and Integrity in Cloud Computing RSA Partial Homomorphic and MD5 Cryptography	RSA homomorphic algorithm.	Efficiency can be improved using different encryption techniques.

4. CONCLUSION:

The security and privacy issues in cloud computing are discussed in this survey paper. Multiple topics such as data confidentiality ,data integrity, data availability, locality etc are discussed along with the methods used to provide data security .A deep analysis of various traditional approaches for authentication and storage mechanism is done which strives to boost up the research ideas and can help in future research work..

5. REFERENCES:

[1] R. Swathi and T. Subha, "Enhancing data storage security in Cloud using Certificate less public auditing," 2017 2nd International Conference on Computing and Communications Technologies(ICCCT),Chennai,2017,pp.348-352.doi: 10.1109/ICCCT2.2017.7972299

[2] S. Bhukya, S. Pabboju and K. V. Sharma, "Data security in cloud computing and out sourced databases," 2016 International Conference on Electrical, Electronics, and Optimization Techniques(ICEEOT),Chennai,2016,pp.2458-2462.doi: 10.1109/ICEEOT.2016.7755135

[3] J. Han, Y. Liu, X. Sun and L. Song, "Enhancing data and privacy security in mobile cloud computing through quantum cryptography," 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, 2016, pp. 398-401.doi: 10.1109/ICSESS.2016.7883094

[4] V. Kulshrestha, S. Verma and C. R. K. Challa, "A comprehensive evaluation of cryptographic algorithms in cloud computing," 2016 International Conference on Inventive Computation Technologies (ICICT),Coimbatore,2016,pp.1-5.doi: 10.1109/INVENTIVE.2016.7823268

[5] T. Subha and S. Jayashri, "Efficient privacy preserving integrity checking model for cloud data storage security," 2016 Eighth International Conference on Advanced Computing (ICoAC),Chennai,2017,pp.55-60.doi: 10.1109/ICoAC.2017.7951745

[6] A U and V. S "A short review on data security and privacy issues in cloud computing," 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC),Bangalore,2016,pp.1-5.doi: 10.1109/ICCTAC.2016.7567341

[7] M. K. Sarkar and S. Kumar, "Ensuring data storage security in cloud computing based on hybrid encryption schemes," 2016 Fourth International Conference on Parallel, Distributed and Grid Computing(PDGC),Waknaghat,2016,pp.320-325.doi: 10.1109/PDGC.2016.7913169

[8] Z. A. Hussien, H. Jin, Z. A. Abduljabbar, M. A. Hussain, S. H. Abbdal and D. Zou, "Scheme for ensuring data security on cloud data storage in a semi-trusted third party auditor," 2015 4th International Conference on Computer Science and Network Technology (ICCSNT), Harbin,2015,pp.1200-1203.doi: 10.1109/ICCSNT.2015.7490948

[9] Goyal, Vikas, and Chander Kant. "An Effective Hybrid Encryption Algorithm for Ensuring Cloud Data Security." Big Data Analytics. Springer, Singapore, 2018. 195-210.

[10] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing."Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. Vol. 1. IEEE, 2012

[11] Dimitrios Zissis, Dimitrios Lekkas, Addressing cloud computing security issues, In Future Generation Computer Systems, Volume 28, Issue 3, 2012, Pages 583-592, ISSN 0167-739X

[12] Shrivas, Arpita, Ojaswi Singh, and Meghna Dubey. "Security concerns and remedies in Cloud Computing." *Electrical, Electronics and Computer Science (SCEECS), 2016 IEEE Students' Conference on*. IEEE, 2016.

[13] https://www.codeproject.com/Articles/1176140/Understanding-Merkle-Trees-Why-use-themwho-uses-t

[14] https://en.wikipedia.org/wiki/Quantum_key_distribution

[15] Agarkhed, Jayashree, and R. Ashalatha. "An efficient auditing scheme for data storage security in cloud." Circuit, Power and Computing Technologies (ICCPCT), 2017 International Conference on. IEEE, 2017.

[16] Yan, Zheng, et al. "Heterogeneous Data Storage Management with Deduplication in Cloud Computing." IEEE Transactions on Big Data (2017).