A NEW MHLA-SHAR BASED, PRIVACY PRESERVING & AUDITING MODEL, FOR CLOUD COMPUTING

Praveen Barode[1], Prof. Kailash Patidar[2]

[1]M. Tech Scholar, [2]M. Tech Guide,
SSSIST Sehore
Department of Computer Science & Engineering

ABSTRACT*: Cloud computing technique serves computing resources such as software, data, hardware, and networks on demand to cloud users. Day by day size of cloud resources and its consumers are increasing rapidly. Cloud computing provides computing services are available 24*7 for cloud users, pay per use basis. Cloud users store their various sensitive and private data on cloud storage servers. So there is a chance of security threads, an unauthorized user can try to access and manipulate data. In this research work, we are presenting, "MHLA-SHAR" a reliable public audit system based on batch auditing system, Improve Key aggregate crypto system, SHA-1 and random masking for data hiding, which performs data auditing on behalf of cloud users. The key point of proposed model is the TPA is stateless, means; TPA does not need to maintain and update state between audits, which is a desirable property especially in the public auditing system. In existing HLA method a new security parameter is added. For the sake of data binding, propose MHLAR scheme involves computationally efficient pairing operation which makes proposed method more efficient and secure. Proposed "MHLA-SHAR" and existing HLA both methods are implemented and various performance and privacy preserving parameters are calculated such as computational time, avalanche effect, and encryption decryption time. An experimental result clearly shows that proposed method performs outstanding over existing method.

***Keywords*- Cloud Computing, Privacy preserving, TPA, MHLA-SHAR and KAC**

IJSDR

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 [1, 4]. The term cloud computing is referred as two terms ,'Cloud' and 'computing', "Cloud" which used here as a "Metaphor" for the technique, "internet" so cloud computing is a "type of web based computing". Cloud computing techniques can dynamically delivers the computing resources and capabilities as a service over the web. It is a new technology of computing in which dynamically scalable and often virtualized resources are provide as a service over the web [7]. Figure 1.1 shows basic cloud computing model.

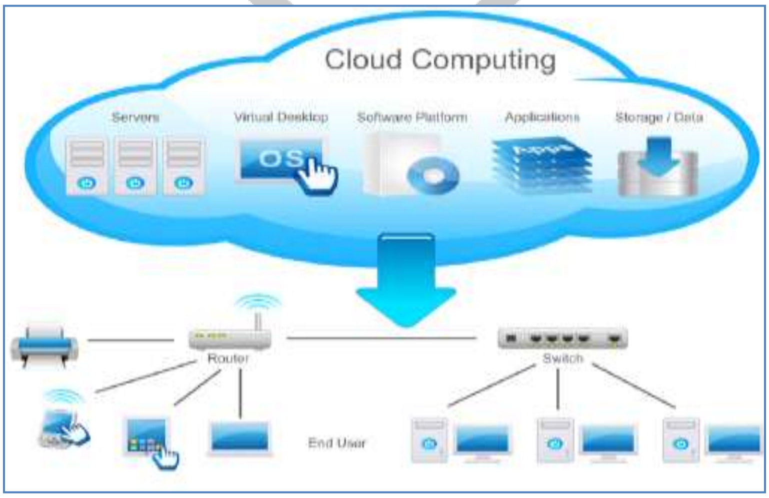


Figure 1.1 Clouds computing basic model

2. CLOUD COMPUTING

"Cloud computing is a large scale based distributed computing technology or paradigm, that is widely driven by economies of scale, in which a pool of computing services are delivered to external cloud users, on demand pay and use basis over the internet, services such as abstracted, virtualized, dynamically scalable managed computing power, storage and platform".

2.1 TYPES OF CLOUD MODELS- There are four types of clouds models private cloud, public cloud, community cloud and hybrid cloud.
1) Private cloud- A private cloud is one, which is setup by single organization and installed services on its own data center.
2) Public cloud- A Public cloud services are offered by third party cloud service providers and involve various computing resource provisioning outside of the cloud user's premises.
3) Community cloud- The Community cloud can offer services to a community or group or the cluster of organizations.
4) Hybrid cloud-A Hybrid cloud provided an integrated service private, public and community cloud.

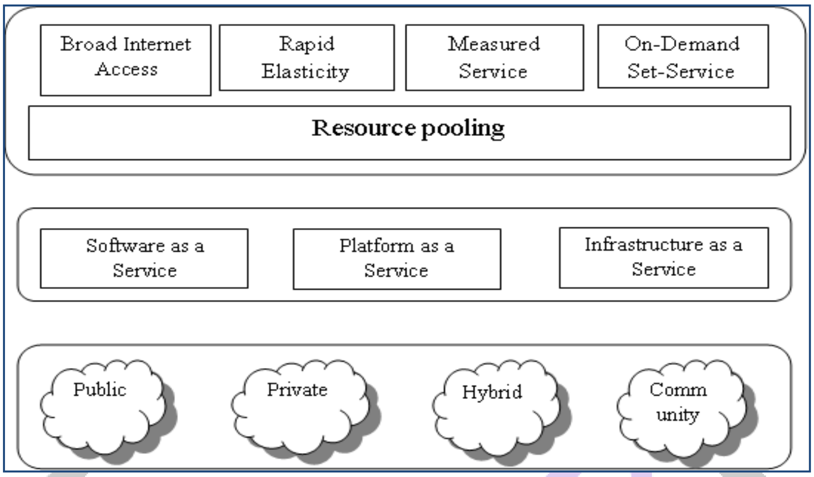


Figure 1.2 Cloud computing architecture model

2.2 CLOUD SERVICES-Cloud provides following four types of services.
1) IaaaS- In infrastructure as a service, cloud provides complete IT infrastructure to cloud user, such as networking, LAN, platform etc.
2) PaaS- In platform as a service, cloud provides provides operating system, platform for development and deployment of applications.
3) SaaS-In software as a service model cloud computing serves essential software's to cloud users.

3. CHALLENGES IN CLOUD COMPUTING

Following Challenges can affect cloud performances-

1. Privacy Preserving- It's very difficult and challenging task to maintain privacy of cloud data. Only an authorize user can access data.
2. Data integrity-Data integrity means data should be correctly stored on the cloud server without any modification and if in any case violations, such as if the data are get lost, modified or compromised can be detected. It must remain the same state; because here the integrity of stored data is at on risk in cloud server [7].
3. Less secure auditing-The Third party auditor is a kind of inspector. TPA helps a cloud user to check the data integrity any time on user demand or request [6]. The auditors can easily understand all the security threats and also they know best security practices. The released audit report helps the user to evaluate the risk of their services. This also helps to CSP in improvement of their cloud platform and service quality [8].
4. Load Balancing- Another challenge in cloud computing is efficient load distributions among various resources.

4. PROPOSED "MHLA-SHAR" MODEL

In this paper we are presenting Modified HLA method with random masking ("MHLA-SHAR") for privacy preserving in cloud computing. In modern cryptography, we often study a fundamental basic problem about leveraging the secrecy of data or a small piece of knowledge into the ability to perform cryptographic functions such as encryption, authentication, multiple times. In this work, we are presenting how to make a decryption key more powerful than existing; in such as way by that it allows decryption of multiple cipher texts, without increasing its size. We solve this new issue by introducing a public-key encryption which we call key-aggregate cryptosystem (KAC).

TPA audit system required steps for auditing the data-

1. User outsource encrypting data at the CS. Encryption perform by improve HLA and KAC algorithm.
2. User requesting to TPA for auditing the data.
3. User sending the public key to TPA for auditing purpose.
4. TPA stores that public key for auditing the file.

5. For auditing TPA send the challenge to CSP
6. CSP send the response of the challenge to TPA.
7. TPA audit result by match the hash value.
8. TPA sends the audit result to user.

In our model, we assume that the point to point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead. Proposed model is based on following two experimental setups-

I First Module- User Share his data to another authorize user or delegate by KAC protocol- In this scenario user can store his encrypted data (CH) in cloud storage area by their user assign an authority to accessing the data by the KAC protocol which generate a fix size key for decryption of the message (M).

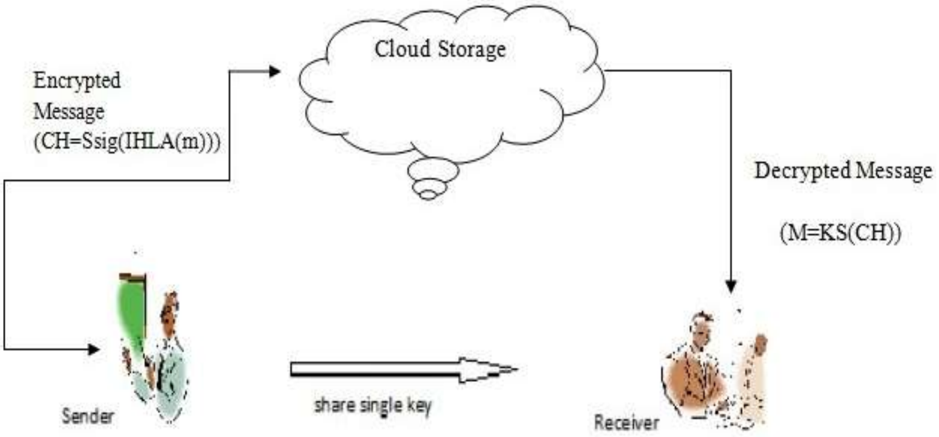


Figure 4.1 KAC framework

II Second Module- User request to TPA for auditing the file by proposed MHLA-SHAR algorithm**.**

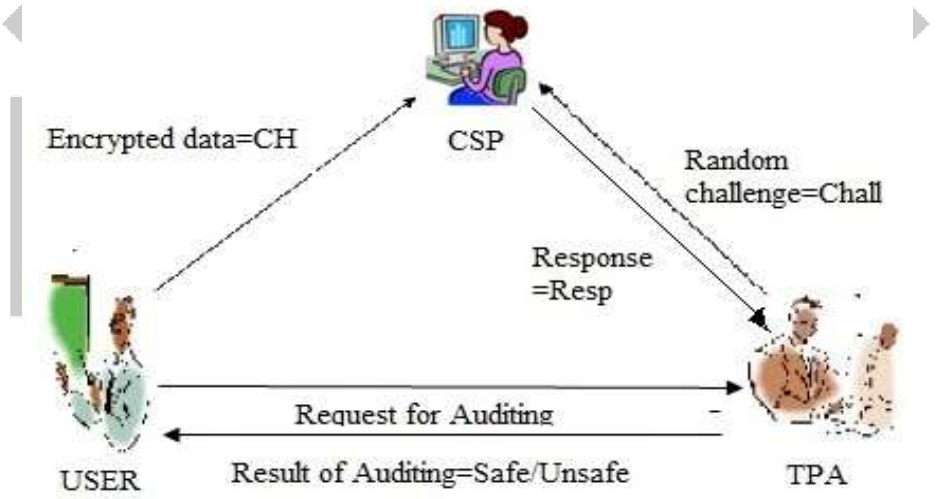


Figure 4.2 Auditing process for proposed system

5. EXPERIMENTAL RESULTS AND COMPARISONS

5.1 COMPARISON PARAMETERS -Following comparison parameters are calculated for existing and proposed system

1. Encryption and Decryption time-Total time which requires to encrypt a plain text message in to its equivalent cipher text are called encryption time and time that requires to converts a cipher text message in to its equivalent plain text text are called decrypt a cipher text. Less encryption and decryption time for a method shows better performance.

2. Brute force attack – Strengths of cipher text are measured by brute force attack. In this attack, attackers apply all the permutation and combination logics to break a plain text message. Higher degree or time to break cipher shows better performance.

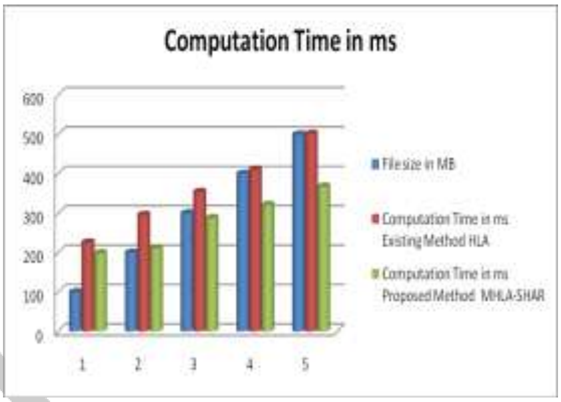
3. Avalanche Effect- In cryptography, the **avalanche effect** refers to an attractive property of block ciphers and cryptographic hash functions algorithms. The **avalanche effect** is satisfied if: The output changes significantly (e.g., half the output bits flip) as a result of a slight change in input (e.g., flipping a single bit), the **avalanche effect** is a desirable effect: it means that a very small change in the input will lead to a very big change in the output.

4. TPA Computational Time- Total time consumes during auditing process. It is the amount of time for which a server was used for processing a file which is stored in cloud server. Less TPA computational times for auditing of a file or data shows better performance of the cloud system.
5. Key Size-The size of an aggregate key which is used at decryption level.

5.2 RESULT ANALYSIS- Following results are calculated for existing and proposed methods.

1. Storage Computational Time- Computational Time are calculated with different file sizes such as 100 MB, 200 MB, 300 MB, 400 MB, 500 MB. Following results are calculated for existing and proposed methods.

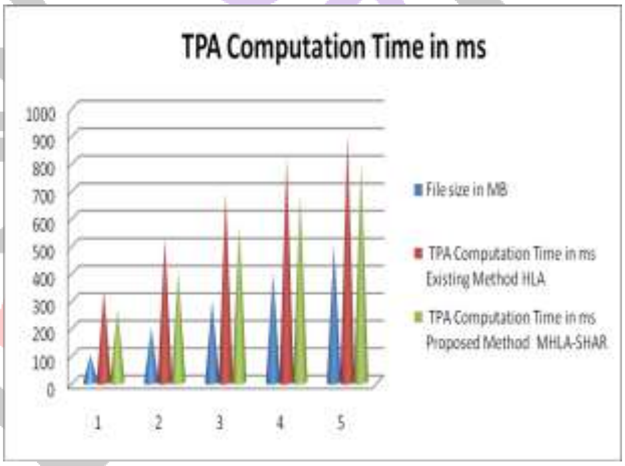
File size in MB	Computation Time in ms	
	Existing Method HLA	Proposed Method MHLA-SHAR
100	225.98	198.77
200	295.88	211.33
300	354.18	287.66
400	411.22	321.1
500	501.97	367.82



Influence- Above results clearly shows computation time of various file of size 100 to 500 MB for existing HLA and proposed MHLA-SHAR method. Results clearly show that proposed method takes less time as compared to existing. Less computational time for a method shows better performance.

2. TPA Computational Time- TPA Computational Times are calculated with different file sizes such as 100 MB, 200 MB, 300 MB, 400 MB, and 500 MB. Following results are calculated for existing and proposed methods.

File size in MB	TPA Computation Time in ms	
	Existing Method HLA	Proposed Method MHLA-SHAR
100	**335.11**	**267.88**
200	**524.22**	**405.88**
300	**688.97**	**574.22**
400	**816.33**	**687.99**
500	**902.45**	**798.99**

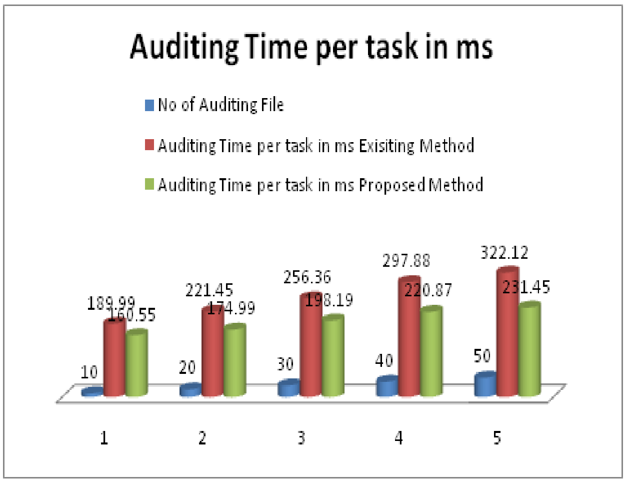


Influence- Above results clearly shows TPA computation time of various file of size 100 to 500 MB for existing HLA and proposed MHLA-SHAR method. Results clearly show that proposed method takes less time as compared to existing. Less TPA computational time shows better performance.

3. Batch Auditing Time – Batch auditing times are calculated for existing and proposed methods. For auditing batch of 10, 20,30,40,50 file are used for auditing.

No of Auditing File	Auditing Time per task in ms	
	Existing Method	Proposed Method
10	189.99	160.55
20	221.45	174.99
30	256.36	198.19
40	297.88	220.87

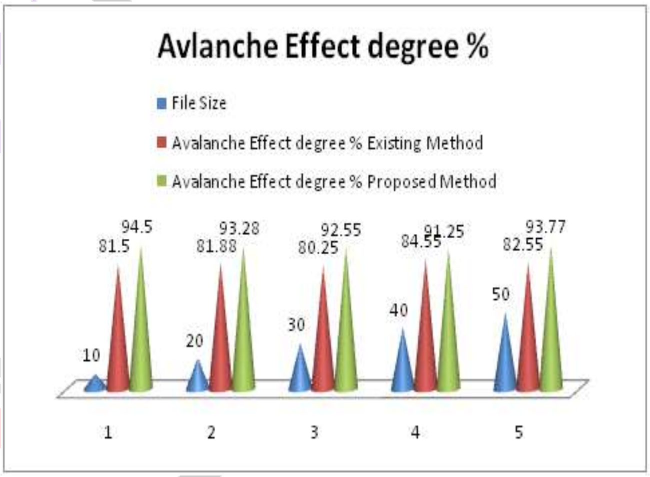
50	322.12	231.45



Influence- Above results clearly shows Batch auditing time of various auditing files such as 10, 20,30,40,50 of various sizes for HLA and proposed MHLA-SHAR method. Results clearly show that proposed method takes less time as compared to existing. Less auditing time shows better performance.

4 Avalanche Effect degree- TPA Computational Times are calculated with different file sizes such as 100 MB, 200 MB, 300 MB, 400 MB, and 500 MB. In plain text file 10 characters are changes.

File Size	Avalanche Effect degree %	
	Existing Method	Proposed Method
10	81.5	94.5
20	81.88	93.28
30	80.25	92.55
40	84.55	91.25
50	82.55	93.77



Influence- Above results clearly shows Batch auditing time of various auditing files such as 10, 20,30,40,50 of various sizes for HLA and proposed MHLA-SHAR method. Results clearly show that proposed method takes less time as compared to existing. Less auditing time shows better performance.

6. CONCLUSION AND FUTURE WORK

Data security plays a vital role in cloud performance and reliability. Cloud user stores their sensitive and private data on cloud server so it's necessary for cloud service provide to maintain data privacy and integrity. In this research work we have presents a new framework by using "MHLA-SHAR" a reliable public audit system for cloud computing. Proposed system is based on batch auditing system, Improve Key aggregate crypto system, SHA-1 and random masking for data hiding, which performs data auditing on behalf of cloud users. The key point of proposed model is the TPA is stateless, means; TPA does not need to maintain and update state between audits, which is a desirable property especially in the public auditing system.

FUTURE WORK-The included support for the choice of cloud providers is limited and very basic, but the framework can be extended to support new providers. Further in the current implementation the organizations have to maintain an application at the clouds that will perform the updating procedure. The framework can be developed in a manner such that the providers can easily integrate it with their platform. Moreover working with encrypted data is computation intensive and expensive in terms of space complexity, performance speed of data processing options in the cloud can be applied for better performance. With reference to cryptographic techniques, the proposed approach using newer homomorphic cryptosystems having additive homomorphic, can be explored for performance benefits

REFERENCES

[1] Swapnali More, Sangita Chaudhari,"Third Party Public Auditing scheme for Cloud Storage", 7th International Conference on Communication, Computing and Virtualization, Science direct, 2016, pp 69-76.

[2] Cong wang, Qian Wang , Kui Ren, Wenjing Lou, " Privacy Preserving Public Auditing for secure cloud data storage", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013, PP 362-375.

[3] Nivedita Shimbre, Prof. Priya Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm", International Conference on Computing Communication Control and Automation, 2015, pp 35-39.

[4] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jinaying Zhou and Robert H. Deng "Key aggregate cryptosystem for scalable data sharing in cloud storage" IEEE transactions on parallel and distributed systems, vol:25 issue 2, year 2014

[5] Tamal Kanti Chakraborty, Anil Dhami, Prakhar Bansal and Tripti, "Enhanced Public Audit ability & Secure Data Storage in Cloud Computing", IJCA 2015, Vol 8 Issue 7, PP 129-135.

[6] S.Hemalatha, Dr. R.Manickachezian, "Dynamic auditing protocol using improved RSA and CBDH for cloud data storage", IEEE conference Co-Comoeo 2014, PP 222-228.

[7] Q. Wang, C. wang, J.Li,K. Ren, W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing", ICCOEA, IEEE conference, 2014, PP 345-351.

[8] Jia Xu, "Auditing the Auditor: Secure Delegation of Auditing Operation over Cloud Storage", ACM, 2014, PP 333-339.

[9] Prabodh S. Nimat, Prof. A. R. Itkikar, "Efficient Data Sharing In Cloud With Third Party Auditor: A Review Study", Journal of Engineering, Computers & Applied Sciences (JEC&AS), ISSN No: 2319-5606, Volume 2, No.6, May 2013, PP 1-3

[10] R.K.Ramesh , P.Vinoth Kumar and R.Jegadeesan [10]- In this research paper authors presented, "NTH Third party auditing for data integrity in cloud".

[11] Abhishek Mohta and Lalit Kumar Awasthi , "Cloud Data Security while using Third Party Auditor", International Journal of Scientific & Engineering Research, ISSN 2229-5518 ,Volume 3, Issue 6, June-2012 , PP 221-226.

[12] 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.

[13] Vijayaraghavan U, Madonna Arieth R, Geethanjali," Proof of Retrivability: A Third Party Auditor Using Cloud", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 7, July 2013, PP 290-294.

[14] Renuka Goyal, Navjot Sidhu, "Third Party Auditor: An Integrity Checking Technique for Client Data Security in Cloud Computing", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 4526-4530.

[15] Patel Himani Atulkumar, Patel Srushti Hasmukhbhai, "Cloud Model with TPA (Third Party Auditor)", IJREAT International Journal of Research in Engineering & Advanced Technology, ISSN: 2320 - 8791,Volume 1, Issue 1, March, 2013,PP 101-103.

[16] Ashish Bhagat, Ravi Kant Sahu, "Cloud Data Security while using Third Party Auditor", International Journal of Computer Applications (0975 – 8887) Volume 70– No.16, May 2013, 9-14.

[17] Ms. A. Christy Sharmila, Mr, T. Darney Tressiline "Cloud audit service outsourcing by using KAC for data storage security" International journal of engineering research and applications (IJERA)ISSN:2248-9622 International conference on humming bird 01st march 2014).