Privacy Preserving in TPA using Blowfish Encryption and Shamir's Secret Sharing for Secure Cloud

Dr. Anjana Pandey[1] Pritam Khatarkar[2]
[1,2]Department of Information Technology
[1,2]Institute of Technology, DDIPG RGPV, Bhopal, India

Abstract— Today, the market of Cloud Computing is developing at a fast. Everybody has their information over cloud which gives the facility to move anyplace and get to the information whenever. Distributed computing is a developing innovation in the field of data innovation. Pretty much Cloud figuring portrays very adaptable processing assets provided as an external administration through web on pay-as-ease of use premise. Distributed computing has been imagined as the cutting edge engineering of IT Enterprise. It moves the application programming and databases to the concentrated substantial data centers, where the administration of the information and administrations may not be completely dependable. This one of a kind worldview achieves numerous new security challenges, which have not been surely knew. This work thinks about the issue of guaranteeing the respectability of information storage in Cloud Computing. In this paper we proposed a novel way to deal with accomplish the protection privacy preserving cloud information evaluating framework by combining distinctive techniques. We utilized Shamir's secret sharing Algorithm for secure key sharing and verification scheme. Hash Key is utilized to check the honesty of information and Blowfish Algorithm utilized for encryption explanation behind enhancing information security and effectiveness.

Keywords: Cloud Computing, TPA, Data Encryption, Cloud Security, Blowfish Algorithm and Shamir's Secret Sharing

I. INTRODUCTION

Distributed computing is an inventive innovation that is upsetting the way we do processing. The key idea of distributed computing is that you don't purchase the equipment, or even the product, you require any longer, rather you lease some computational power, stockpiling, databases, and some other asset you require by a supplier as indicated by a compensation as-you-go display, making your speculation littler and arranged to operations as opposed to resources procurement. Be that as it may, there is significantly more than that, obviously, and there are a wide range of ways how this approach can be placed in action. Cloud figuring is a model for empowering all over the place, very much situated, on-request arranging access to a mutual pool of configurable processing assets (e.g., systems, servers, applications, and administrations). Principally clients can withdraw its support administrations to cloud specialist organization that is master in giving learning and furthermore keeps up its huge measure assets. Much the same as a twofold bladed sword, distributed computing likewise acquires numerous new security challenges on ensuring the respectability and protection of clients' information in the cloud. To address these issues, our work uses the system of mystery key based symmetric key cryptography which empowers TPA to play out the examining without requesting the neighborhood duplicate of client's put away information and in this way seriously finds the transmission and calculation overhead when contrasted with the direct information inspecting approaches. Accordingly incorporating the encryption with hashing, our convention ensures that the TPA couldn't take in any information about the information content put away in the cloud server amid the proficient examining process. Distributed computing, which gives Internet based administration and utilization of PC innovation. This is less expensive and more solid processors, together with the product as an administration (SaaS) figuring engineering, are changing information into server farms on gigantic scale. The expanding system and adaptable system associations influence it even conceivable those clients to would now be able to utilize top notch administrations from information and gives remote on server farms. Putting away information into the cloud offers extraordinary help to clients since they don't need to think about the issues of equipment. While these webs based online administrations do give gigantic measures of storage room and adaptable figuring assets, this registering stage move, however maintains a strategic distance from the duty of neighborhood machines for information support in the meantime. Accordingly, clients are at the enthusiasm of their cloud specialist organizations for the accessibility and trustworthiness of their information the one hand; despite the fact that the cloud administrations are significantly more effective and solid than individualized computing gadgets and wide scope of both interior and outer dangers for information uprightness still exist. Cases of blackouts and information misfortune episodes of important distributed storage administrations show up every now and then. Then again, since clients may not keep a nearby duplicate of outsourced information, there exist different motivating forces for cloud specialist organizations (CSP) to act unfaithfully towards the cloud clients with respect to the status of their outsourced information. Our work is among the initial couple of ones in this field to consider dispersed information storage security in Cloud Computing.

II. RELATED WORK

Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou [01], In this paper they explain, Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check

the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new Vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Imran Ahmad, Prof. Hitesh Gupta [02], In this paper they explain, Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and Services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

Ankush R. Nistane, Shubhangi Sapkal, Dr. R. R. Deshmukh [03], Using cloud services, anyone can remotely store their data and can have the on-demand high quality applications and services from a shared pool of computing resources, without the burden of local data storage and maintenance. Cloud is a commonplace for storing data as well as sharing of that data. However, preserving the privacy and maintaining integrity of data during public auditing remains to be an open challenge. In this paper, we introducing a third party auditor (TPA), which will keep track of all the files along with their integrity. The task of TPA is to verify the data, so that the user will be worry-free. Verification of data is done on the aggregate authenticators sent by the user and Cloud Service Provider (CSP). For this, we propose a secure cloud storage system which supports privacy-preserving public auditing and blockless data verification over the cloud. Jyoti R Bolannavar1 [04], In this paper thy explain, Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public audit ability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Salve Bhagyashri, Prof. Y.B.Gurav [05], In this paper they explain, By using Cloud storage, users can access applications, services, software whenever they requires over the internet. Users can put their data remotely to cloud storage and get benefit of on-demand services and application from the resources. The cloud must have to ensure data integrity and security of data of user. The issue about cloud storage is integrity and privacy of data of user can arise. To maintain to overkill this issue here, we are giving public auditing process for cloud storage that users can make use of a third-party auditor (TPA) to check the integrity of data. Not only verification of data integrity, the proposed system also supports data dynamics. The work that has been done in this line lacks data dynamics and true public auditability. The auditing task monitors data modifications, insertions and deletions. The proposed system is capable of supporting public auditability, data dynamics and Multiple TPA are used for the auditing process. We also extend our concept to ring signatures in which HARS scheme is used. Merkle Hash Tree is used to improve block level authentication. Further we extend our result to enable the TPA to perform audits for multiple users simultaneously through Batch auditing.

Sathiskumar R, Dr.Jeberson Retnaraj [06], In this paper they explain, Cloud storage provides users to easily store their data and enjoy the good quality cloud applications need not install in local hardware and software system. So benefits are clear, such a service is also gives users' physical control of their outsourced data, which provides control over security problems towards the correctness of the storage data in the cloud. In order to do this new problem and further achieve secure and dependable cloud storage services. The main goal of cloud computing concept is to secure, protect the data and the processes which come under the property of users. The security of cloud computing environment is an exclusive research area which requires further development from both the academic and research communities. In cloud environment the computing resources are under the control of service provider, the third party auditor ensures the data integrity over out sourced data. In this paper we proposed Encryption and Proxy encryption algorithm to protect the privacy and integrity of outsourced data in cloud Environments.

III. PROPOSED METHODOLOGY

In this paper we proposed a novel scheme by consolidating different methods to accomplish privacy preserving public

auditing for TPA. Methods we utilized as a part of this paper are, we utilized Authentication convention for cloud computing for more secure design which is finished by SSL already. We used Shamir's secret sharing algorithm for secure key sharing and verification scheme. At the point when any request comes from customer for information (data sharing) on the cloud we validate the customer utilizing Shamir's secret sharing. Hash Key is used to check the integrity of data. And we used Blowfish Algorithm for encryption reason for enhancing data security and efficiency. Data traveling over cloud is encrypted using blowfish algorithm. The proposed system specifies that user can access the data on a cloud without worrying about the security and integrity of the data.

IV. PROPOSED FRAMEWORK

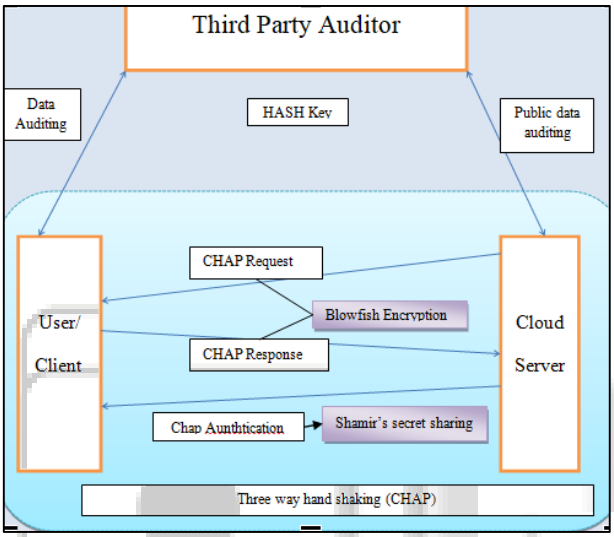

Fig. 3.1: Flowchart of proposed system

CHAP is a protocol basically known for authenticate the legitimate remote users. It is utilized for the different type of validation of remote users. Whenever a client send a request for upload or download the data from server the authentication of user is first checked and then Blowfish and Shamir's Secret Sharing is utilized for encryption & decryption and key sharing purpose.

V. RESULT

VI. CONCLUSION

This paper investigated information storage rightness issue in context of distributed computing. This paper proposed a secure mechanism for trusted and secure information storage model with data security and integrity check. The algorithms utilized by this framework turn out helpful to decrease computational cost for the clients who have information security issue over cloud information storage. TPA can audit the data on the server, and can ensure the security in data correspondence. The cloud server customers have assured for the authenticity of their information by executing proposed system. Along these lines we can secure our data sharing over the cloud servers using proposed structure.

REFERENCES

[1] Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Computers, Volume: 62, Issue: 2, 20 December 2011, DOI: 10.1109/TC.2011.245

[2] Imran Ahmad, Prof. Hitesh Gupta, "Privacy-Preserving Public Auditing & Data Intrgrity for Secure Cloud Storage", International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV 100,

[3] Ankush R. Nistane, Shubhangi Sapkal, Dr. R. R. Deshmukh, "Privacy Preserving Public Auditing and Data Integrity for Secure Cloud Storage Using Third Party Auditor", International Journal of Advanced Engineering, Management and Science (IJAEMS), Vol-2,Issue-2,February 2016,

[4] Jyoti R Bolannavar, "Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage", International Journal of Scientific Engineering and Research (IJSER), ISSN (Online): 2347-3878 Volume 2 Issue 6, June 2014,

[5] Salve Bhagyashri, Prof. Y.B.Gurav, "Privacy-Preserving Public Auditing For Secure Cloud Storage", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. III (Jul – Aug. 2014), PP 33-38,

[6] Sathiskumar R, Dr.Jeberson Retnaraj, "Secure Privacy Preserving Public Auditing for Cloud storage", International Journal of Innovative Research in Science, Engineering and Technology An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014,

[7] Tejashree Paigude, Prof. T. A. Chavan, "A survey on Privacy Preserving Public Auditing for Data Storage Security", International Journal of Computer Trends and Technology, volume 4, Issue 3 2013, ISSN: 2231-2803,

[8] Vikram.J, M.Kalimuthu, "A Comparative Study on Privacy-Preserving Public Auditing for Secure Cloud Storage", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 11, November 2014,

