International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 5 Ver. III || May 2018 || PP 66-71

Privacy Preserving In Tpa Using Blowfish Encryption And Shamir's Secret Sharing For Secure Cloud

Sneha Khemani and Payal Awwal
Govt. Women's Engineering College, Ajmer
Corresponding Auther: Sneha Khemani

Abstract:*Now a day, the requirement for cloud information stockpiling is high-on-request as clients can remotely store their information and recover it from anyplace. This can prompted the weakness towards the cloud client's information and protection as these data's are going over the cloud. A system should be produced where client ought to have the capacity to simply utilize the distributed storage without pondering the defenselessness of their information and security. In this manner, the significance of public auditing capacity of distributed storage is raised where client can depend on a TPA to check the protection and trustworthiness of outsourced information. This paper proposed a secured way to deal with accomplish the protection safeguarding in distributed storage utilizing Shamir's secret sharing, Hash Key and Blowfish encryption calculation. Shamir's secret sharing Algorithm utilized for secure key sharing and affirmation plan, Hash Key is utilized to check the validity of information and Blowfish Algorithm utilized for encryption elucidation behind enhancing information security and viability.*

Date of Submission: 07-05-2018 Date of acceptance: 22-05-2018

I. Introduction:

Distributed computing is a model for engaging everywhere, particularly arranged, on-ask for orchestrating access to a common pool of configurable processing resources (e.g., frameworks, servers, applications, and organizations). This encourages clients to store their information over cloud since they don't need to think about the issues of hardware problem. The need of Cloud Computing is expanding quickly since everyone has their data over cloud which gives the ability to move wherever and get to the data at whatever point. Cloud computing is a creating advancement in the field of information development. Essentially Cloud figuring depicts extremely versatile preparing resources gave as an outer organization through web on pay-as-usability preface. Distributed computing has been imagined as the cutting edge engineering of IT Enterprise. It moves the application programming and databases to the concentrated generous datacenters, where the organization of the data and organizations may not be totally reliable. A protection safeguarding open evaluating framework for information stockpiling security in distributed computing is the homomorphic straight authenticator and irregular veiling to ensure that the TPA would not take in any learning about the information content put away on the cloud server amid the effective reviewing process. It not just takes out the weight of cloud client from the dull and potentially costly auditing task, yet in addition reduces the clients' dread of their outsourced information spillage.

Blowfish Encryption Algorithm

Blowfish is a symmetric square figure that can be utilized as a drop-in swap for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it perfect for both local and exportable utilize. Blowfish was planned in 1993 by Bruce Schneier as a quick, free contrasting option to existing encryption calculations. From that point forward it has been investigated significantly, and it is gradually picking up acknowledgment as a solid encryption calculation. Blowfish is unpatented and permit free, and is accessible free for all employments.

Blowfish is incorporated into countless suites and encryption items, including SplashID. Blowfish's security has been widely verified. As an open area figure, Blowfish has been liable to a lot of cryptanalysis, and full Blowfish encryption has never been broken. Blowfish is likewise one of the quickest piece figures in broad daylight utilize, making it perfect for an item like SplashID that capacities on a wide assortment of processors found in cell phones and in addition in scratch pad and personal computers.

Schneier planned Blowfish as a broadly useful calculation, expected as a swap for the maturing DES and free of the issues related with different calculations.

Blowfish is a symmetric block encryption algorithm designed in consideration with,

- **Fast:** It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.

- **Compact:** It can run in less than 5K of memory.
- **Simple:** It uses addition, XOR, lookup table with 32-bit operands.
- **Secure:** The key length is variable, it can be in the range of 32~448 bits: default 128 bits key length.

Shamir's Secret Sharing

A **secret sharing scheme** is a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.

More formally, in a secret sharing scheme there are one dealer and n players. The dealer gives a secret to the players, but only when specific conditions are fulfilled. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of less than t players can. Such a system is called a (t,n)-threshold scheme.

A popular technique to implement threshold schemes uses polynomial interpolation("Lagrange interpolation"). This method was invented by Adi Shamir in 1979.

Secret

Secret is a secret message or number that you want to share with others securely.

Share

Share is a piece of secret. Secret is divided into pieces and each piece is called share. It is computed from given secret. In order to recover the secret, you need to get certain numbers of shares.

Threshold

Threshold is the number of shares you need at least in order to recover your secret. You can restore your secret only when you have more than or equal to the number of threshold.

II. Related Work:

Cong Wang , Sherman S.-M. Chow, Qian Wang,Kui Ren, and **Wenjing Lou [01],** In this paper they explain, UsingCloudStorage,userscanremotelystoretheirdataandenjoytheon-demandhighqualityapplicationsand servicesfromasharedpoolofconfigurablecomputingresources,withouttheburdenoflocaldatastorageandmaintenance .However,thefactthatusersnolongerhavephysical possession oftheoutsourced datamakesthedataintegrityprotection in CloudComputinga formidabletask, especially foruserswithconstrainedcomputingresources.Moreover,users shouldbeabletojustusethecloudstorageasifitislocal,withoutworryingabouttheneedtoverifyitsintegrity.Thus,enablin gpublicauditabilityforcloudstorageisofcriticalimportancesothatuserscanresorttoathirdpartyauditor(TPA)tocheckth eintegrityofoutsourceddataandbeworryfree.TosecurelyintroduceaneffectiveTPA,theauditingprocessshouldbringin nonewVulnerabilitiestowardsuserdataprivacy,andintroducenoadditionalonlineburdentouser.Inthispaper,weproposeas ecurecloudstoragesystemsupportingprivacypreservingpublicauditing.WefurtherextendourresulttoenabletheTPAto performauditsformultipleuserssimultaneouslyandefficiently.Extensivesecurityandperformanceanalysisshowthepr oposedschemesareprovablysecure andhighlyefficient.

S.Ezhil Arasu, B.Gowri, S.Ananthi [02], In this paper they explain, Cloud computing is the arising technology to minimize the user burden in the updation of data in business using internet. Instead of local data storage and maintenance, the user is assisted with the cloud storage so that the user can remotely store their data and enjoy the on-demand high quality application from a shared pool of resources. The data stored must be protected in the cloud storage. To enhance the correctness of data, auditing process is done which is carried out by TPA (Third Party Auditor). The TPA must be efficient to audit without demanding the local copy of data. In this paper we have proposed a method that uses the keyed Hash Message Authentication Code (HMAC) with the Homomorphic tokens to enhance the security of TPA.

Hongyu Liu,Zahra Davar [03], In this paper they explain, Cloud storage has a long string of merits but at the same time, poses many challenges on data integrity and privacy. A cloud data auditing protocol, which enables a cloud server to prove the integrity of stored files to a verifier, is a powerful tool for secure cloud storage. Wang et al. proposed a privacy-preserving public auditing protocol; however, Worku et al. found the protocol is seriously insecure and proposed an improvement to remedy the weakness. In this paper, unfortunately, we demonstrate that the new protocol due to Worku et al. fails to achieve soundness and obtains merely limited privacy. Specifically, we show even deleting all the files of a data owner, a malicious cloud server is able to generate a response to a challenge without being caught by TPA in their enhanced but unrealistic security model. Worse still, the protocol is insecure even in a correct security model. For privacy, a dishonest verifier can tell which file is stored on the cloud. Solutions to efficient public auditing mechanisms with perfect privacy protection are still worth exploring.

Vitthal Sadashiv Gutte, Prof. Priya Deshpande [04], In this paper they explain, with the advancement of cloud computing and storage technology, large-scale databases are being exponentially generated today. Storage management systems to cloud it still faces a number of fundamental and critical challenges, among which storage space and security is the top concern. To ensure the correctness of user and user's data in the cloud, we

propose third party authentication system. In addition to simplified data storage and secure data acquisition. Finally we will perform security and performance analysis which shows that the proposed scheme is highly efficient for maintaining secure data storage and acquisition.

Ms.Madhuri B.Patil, Mr N. Aravind Kumar [05],this paper they explain, Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data rather than a local server or a personal computer. The privacy preserving supports the public auditing without the retrieval access of entire data blocks. The integrity of data in cloud storage, however, is subject to skepticism and scrutiny, as data stored in an untrusted cloud can easily be lost or corrupted, due to hardware failures and human errors. To protect the integrity of cloud data, it is best to perform public auditing by introducing a third party auditor (TPA), who offers its auditing service with more powerful computation and communication abilities than regular users. In this paper, we propose Oruta, a new privacy preserving public auditing mechanism for shared data in an untrusted cloud. In Oruta, we utilize ring signatures to construct homomorphic authenticators, so that the third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data — while the identity of the signer on each block in shared data is kept private from the TPA. We only consider how to audit the integrity of shared data in the cloud with static groups.

Yogesh Shinde,Dr. D. Y. Patil [06], In this paper they explain, Cloud Computing is a utility computing such as Pay-as-you-go computing, Illusion of Infinite Resources, No Upfront Cost, Fine grained billing. User's store their large amount of data on a cloud severs at remote place without worryingabout Storage Correctness as well as information Integrity. Sothat users can option to a Third Party Auditor (TPA) to testthe data integrity and be worry-free because user does not physical present at all time. The Third Party Auditor (TPA) performs audits for multiple cloud users simultaneouslyand efficiently.In this paper, proposed scheme contain data files dividedinto small block technique. Which ensure cloud storage security, integrity? To increase the user level security we proposed One Time Password (OTP) at the time of file uploading. Partitioning process implemented at TPA side. TPA performs operation like data files divided into small part of block, take hash of each block, each block Encrypt using cryptographic algorithm.

Yenduva Venkata Mukesh Naidu, Panuganti Ravi [07], In this paper they explain, In the cloud server, cloud users can store their data and high quality of services and applications.in the cloud environment they were used configurable computing resources, without the problem of local data storage and maintenance problems.Cloud users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task.if we not providing the integrity protection should be able to just use the cloud storage as if it is local. Public auditability is mandatory for cloud storage.so users can approach to a third-party auditor (TPA) to check the integrity of outsourced data than they are not worry about the cloud protection. The auditing process should bring in no new vulnerabilities toward clouduser data and we can reduce the additional online burden to the 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.

Rohini Kadlag, Rohit Devikar [08], In this paper they explain,Cloud Computing is nothing but specific style of computing where everything from computing power to infrastructure, business apps are provided "as a service". In cloud, shared resources, softwares and information is provided as a metered service over the network. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. In this paper we are extending the previous system by using automatic blocker for privacy preserving public auditing for data storage security in cloud computing. We utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique and automatic blocker. In particular, to achieve efficient data dynamics, we improve the existing proof of storage models by manipulating the block tag authentication. Thus, TPA eliminates the involvement of the client through the auditing of whether his Data stored in the Cloud are indeed intact, which can be important in achieving economies of scale For Cloud Computing.

Mr. V. Sajeev, Mrs. R. Gowthamani [09], In this paper they explain, Cloud computing is the long dreamed vision where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, the burden of local data storage and maintenance can be relieved from users. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage

without demanding the separate copy of data as local, and introduce no additional on-line burden to the cloud user 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper we propose a system of auditing using BAC (Block Authentication Code).

Poli Reddy, B. Bala Krishna [10], In This paper they explain, during this paper, we advise a privacy-preserving public auditing system for knowledge storage safety in cloud computing. victimization cloud storage, users will tenuously store their knowledge and revel in the on-demand high-quality applications and services from a shared pool of configurable dividing resources, while not the burden of native knowledge storage and preservation. However, the actual fact that users not have physical possession of the outsourced knowledge makes the info integrity protection in cloud computing a tough task, expressly for users with forced computing possessions. Moreover, users ought to be able to simply use the cloud storage as if it's native, while not distressing concerning the requirement to verify its dependability. Thus, facultative public audit ability for cloud storage is of vital importance in order that users will resort to a third-party auditor (TPA) to see the integrity of outsourced knowledge and be worry free. To firmly introduce a lively TPA, the auditing method ought to usher in no new vulnerabilities toward user knowledge privacy, and introduce no any on-line drawback to user. During this paper, we tend to propose a secure cloud storage system supporting privacy-preserving public auditing. We tend to any spread our result to change the TPA to perform audits for multiple users at the same time and with efficiency. General security and performance analysis show the projected schemes square measure demonstrably secure and extremely well-organized. Our primary experiment conducted on Amazon EC2 instance any demonstrates the quick performance of the look.

III. Propsed Methodlolgy:

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. Result Analysis / Implementation:

Figure 4.1 demonstrate the all available functionality for clients like file uploading, data encryption, data download, and view files.

Figure 4.1: - Client Functionalities

Figure 4.2 show the process of file upload, data encryption using blowfish encryption and encrypted file send to cloud.

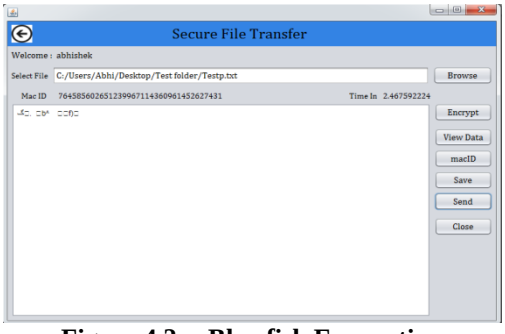

Figure 4.2: - Blowfish Encryption

Figure 4.2 show the process of Shamir's secret key generationfor a selected file and the key is divided based on no of shares and threshold and divided secret/key is send to selected members and these keys will help client later to download the file.

Figure 4.3: - Secret Shamir's generation and sharing

In Figure 4.4 TPA verify the file for download request. When client request a file for downloading, the key access request is also sent to all members to whom the divided Shamir's secret key is sent. If all members approve request then TPA will access to get the entire divided key and assemble it. If the assembled key will match with original Shamir's secret key the file will downloaded at client's resources.

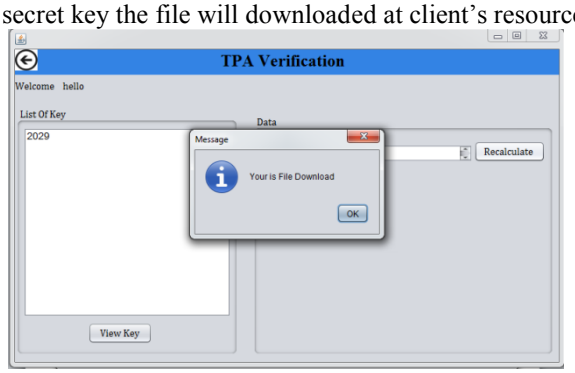

Figure 4.4: - TPA verifying download request

In Figure 4.5, if client's request for file download is approved by TPA the file is available at resource folder. The client selects the downloaded file and decrypts it, after decryption the client will able to view the original uploaded data.

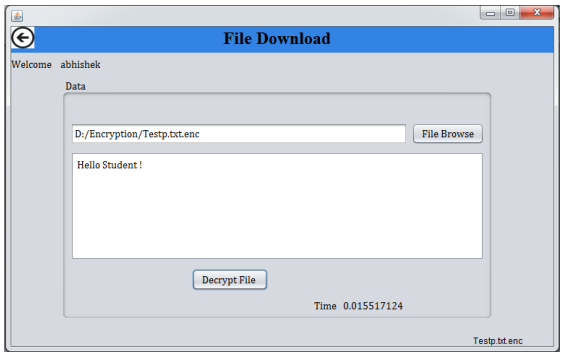

Figure 4.5: - Decryption of Downloaded file

In Figure 4.6, the performance analysis and comparison through a proposed framework Using Blowfish Encryption and Shamir's Secret Sharing for Secure Cloud gives better result comprising more secure, less file access time and better throughput which leads to providing a better and secure cloud service.

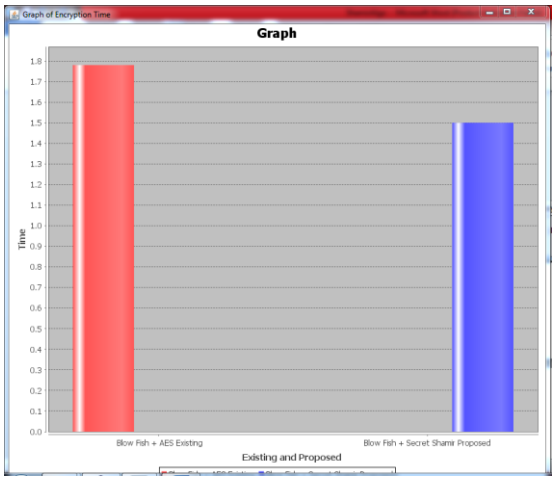

Figure 4.6: - Comparison Graph between Existing System and Proposed System

This comparison graph demonstrates that the proposed framework utilizing Blowfish encryption, TPA and Secret Shamir's key sharing Algorithm can perform better than existing approach in context of privacy preserving.

V. Conclusion

In cloud computing data storage security and integrity is the main issue to be resolved.This paper proposed a framework which is capable of providing secure and trusted mechanism for cloud data security and data integrity. By utilizing this proposed framework one can be assured that their outsourced data will not be vulnerable while the cloud auditing process.Using Shamir's secret sharing to authorize customers, Hash Key for data integrity check and Blowfish Algorithm for data encryption this framework can reduce the computational cost of storage service providers and to ensure the integrity of the Cloud User's data stored in the cloud data centre.

Refrences

[1]. Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou,**"Privacy-PreservingPublicAuditingfor SecureCloudStorage"**, IEEE Transactions on Computers, Volume: 62, Issue: 2, 20 December 2011, DOI: 10.1109/TC.2011.245

[2]. S.Ezhil Arasu, B.Gowri, S.Ananthi, **"Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm",** International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-1, March 2013,

[3]. Hongyu Liu, Zahra Davar, **"Insecurity of an efficient privacy-preserving public auditing scheme for cloud data storage,** Journal of Universal Computer Science, vol. 21, no. 3 (2015),

[4]. Vitthal Sadashiv Gutte, Prof. Priya Deshpande, **"A Survey on Privacy Preserving Technique to Secure Cloud",** International Journal of Software and Web Sciences (IJSWS), ISSN (Print): 2279-0063, February 2015,

[5]. Ms.Madhuri B.Patil, Mr. N. Aravind Kumar**, "Oruta: Public Auditing for Shared Data in the Cloud Storage",**International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842, Issue 6, Volume 2 (June 2015),

[6]. Yogesh Shinde, Dr. D. Y. Patil, **"Privacy Preserving using Data Partitioning Technique for Secure Cloud Storage",**International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 16, April 2015,

[7]. Yenduva Venkata Mukesh Naidu, Panuganti Ravi, **"A Secure Cloud Storage System for Supporting Privacy-PreservingPublic Auditing",** International Journal & Magazine of Engineering, Technology, Management and research, Volume No: 2 (November 2015), Issue No: 11(November),

[8]. Rohini Kadlag, Rohit Devikar, **"A Survey on Automatic Protocol Blocker for Privacy Preserving Public Auditing in Cloud Computing",** International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-3, Issue-12, May 2014,

[9]. Mr. V. Sajeev, Mrs. R. Gowthamani, **"Privacy Preserving Public Auditing in Secured Cloud Storage",** International Journal of Scientific Research Volume: 3 | Issue: 3 | March 2014 • ISSN No 2277 – 8179,

[10]. **Poli Reddy, B. Bala Krishna, "Providing Security and Efficient Privacy-Preserving Public Auditing",** International Journal of Computer Science and Mobile Computing, ISSN 2320–088X, IJCSMC, Vol. 3, Issue. 8, August 2014, pg.526 – 531

Sneha Khemani "Privacy Preserving In Tpa Using Blowfish Encryption And Shamir's Secret Sharing For Secure Cloud "International Journal of Engineering Science Invention (IJESI), vol. 07, no. 05, 2018, pp 66-71