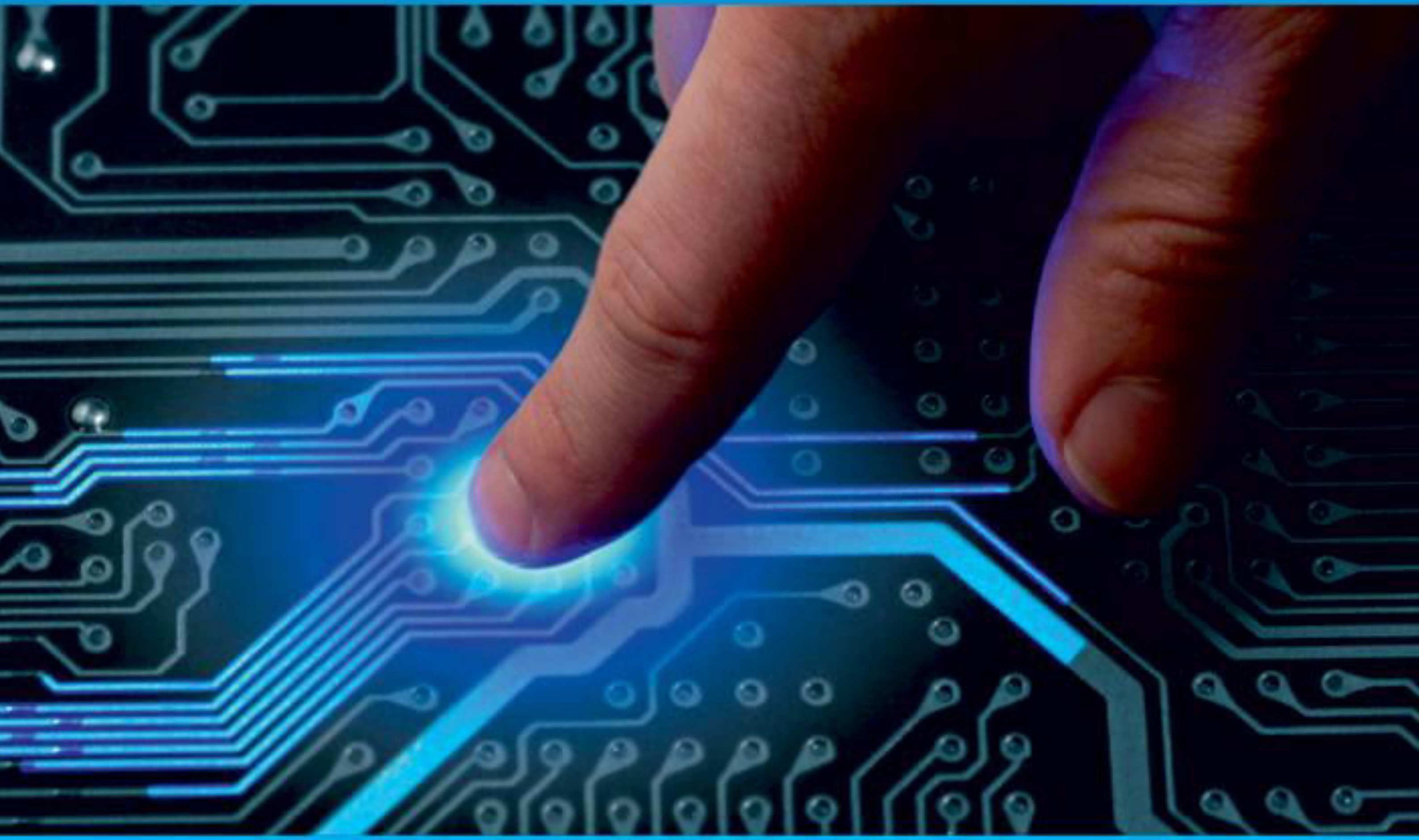
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908035 |

A Cryptographic Technique and TPA based Privacy Preserving using Secret Shamir's Algorithm

Ms.Mrunali S. Kolhe, Prof. Vaishali Londhe

PG Student, Department of Computer Engineering, Yadavrao Tasgaonkar Institute of Engineering and Technology, Maharashtra, India

Professor, Department of Computer Engineering, Yadavrao Tasgaonkar Institute of Engineering and Technology, Maharashtra, India

ABSTRACT: Today Cloud Computing is developing very fast. All users data is stored in the cloud, so the process of retrieve the data and restore the same is much easier than storing the data on physical device. Cloud allows easy to access the data from anywhere but the major challenges in cloud is security and protection of sensitive data. To overcome the security and privacy issues of sensitive information it can be overcome by AES encryption and TPA.

To find a solution of this challenges , this proposed work uses the technique of secret key based symmetric key cryptography which allows TPA to perform the auditing task without demanding local copy of stored data and thus it reduces the risk and make it simple for data auditing approaches. This work thinks about the issue of guaranteeing the respectability of information storage in Cloud Computing. In this paper we proposed a creative way to deal with 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 AES Algorithm utilized for encryption explanation behind enhancing information security and effectiveness.

KEYWORDS: Cloud Computing, TPA, Data Encryption, CHAP,MD5 , Cloud Security, AES Algorithm and Shamir’s Secret Sharing, Cloud Service Provider (CSP)**.**

I. INTRODUCTION

A distributed system allows resource sharing, including software by systems connected to the network. Distributed computing is a framework for engaging all over, organized, on-ask for manage access to a standard pool of configurable processing resources (e.g. frameworks, servers, applications, and organizations). This motivate clients/users to store their information over cloud since they don't need to think about the issues of hardware problem. The requirment of Cloud Computing is increasing fast since all peoples has their data over cloud which gives the ability to move anywhere and get to the data at any place. Originally Cloud figuring represents extremely versatile preparing resources gave as an outer organization through web on pay-as-usability preface. Distributed computing 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 assure that 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.

II. EXISTING SYSTEM

In exsisting system, A scheme Privacy-Preserving Selective Aggregation (PPSA), which encrypts users’ sensitive data to prevent privacy disclosure from both outside analysts and the aggregation service provider, and fully supports selective aggregate functions for online user behavior analysis while guaranteeing differential privacy[5]. The Boneh-Goh-Nissim (BGN) Cryptosystem is a kind of homomorphic cryptosystem which utilizes a bilinear pairing to allow the computation of an unlimited number of homomorphic additions and a single homomorphic multiplication of two ciphertexts. Based on BGN homomorphic cryptosystem, the first system that is able to securely and selectively aggregate user data, making it practical in realistic data analytics. It guarantees strong privacy preservation by utilizing differential privacy mechanism to protect individuals' privacy. In existing system , there is direct contact between user and cloud . Whenever user upload and download file from cloud , attacker can easily access their data by users up address like change users password etc due to direct interaction between cloud and user. Homomorphic alternative of BGN is not semantically Secure and it is less efficient

In proposed system , we add TPA for strong security . When user upload and download data from cloud ,TPA access users MAC id and clouds mac id and compare these id through hash code , so that strong privacy is occurs

III. RELATED WORK

[1] In this paper they explain, Using Cloud Storage, users can remotely store their data and take benifit of on-demand top 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 not have physical possession of the outsourced data makes the info integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be ready to just use the cloud storage as if it's local, without worrying about the necessity to verify its integrity.Thus,enabling public auditability for cloud storage is of critical importance in order that users can resort to a third party auditor (TPA) to see the integrity of outsourced data and be worry free. To securely introduce an efficient TPA, the auditing process should bringing 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.

[2] Using cloud services, anyone can remotely store their data and may have the on demand top quality applications and services from a shared pool of computing resources, without the burden of local data storage and maintenance. Cloud may be a common place for storing data also as sharing of that data. However, preserving the privacy and maintaining integrity of knowledge during public auditing remains to be an open challenge. during this paper, we introducing third party auditor (TPA), which can keep track of all the files along side their integrity. The task of TPA is to verify the info , in order that the user are going to be worry-free. Verification of knowledge is completed on the mixture 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 block less data verification over the cloud.

[3]In this paper they explain, Cloud computing is execute of employing a network of remote servers hosted on internet to store, handle, and process data instead of local server or a private computer. The privacy preserving supports public auditing without the retrieval access of entire data blocks. The integrity of knowledge 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's 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 replacement privacy preserving public auditing mechanism for shared data in an untrusted cloud. In Oruta, we utilize ring signatures to construct homomorphic authenticators, in order that the third party auditor is in a position to verify the integrity of shared data for group of users without retrieving the whole data — while the identity of the signer on each block in shared data is kept private from the TPA. We only consider the way to audit the integrity of shared data within the cloud with static groups.

[4] In this paper, they propose a completely unique privacy-preserving security solution for cloud services. Our solution is predicated on an efficient non bilinear group signature scheme providing the anonymous access to cloud services and shared storage servers. The novel solution offers anonymous authentication for registered users. Thus, users' personal attributes (age, valid registration, successful payment) are often proven without revealing users' identity, and users can use cloud services with none threat of profiling their behavior.

IV. PROPOSED SYSTEM

1. AES-256 Secret Key

AES (Advanced Encryption Standard)Algorithm for encryption reason for enhancing data security and efficiency. Data traveling over online is encrypted using AES algorithm. This algorithm enables to deal with different key sizes such as 128, 192, and 256 bits with 128 bits block cipher[5]. AES is used in many cryptography protocols such as Socket Security Layer (SSL) and Transport Security Layer protocol to provide much more communications security between client and server over the internet[5]. AES 256 bits is safest encryption standard as it have 2^256 unique combinations. 256-bit encryption is so strong. There are many more key combinations can exist in AES-256 and it is very difficult to try many unique combinations to crack the file password.

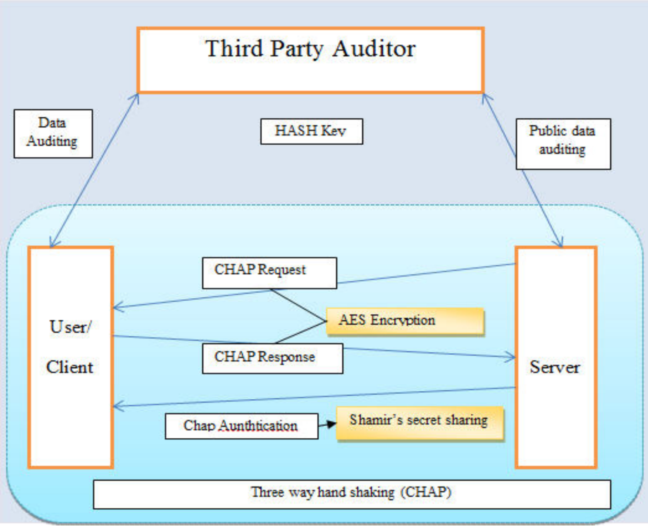


Fig1. Flowchart of proposed system

2. CHAP - Challenge Handshake Authentication Protocol

CHAP is a protocol basically known for authenticate the legitimate remote users. CHAP is MD5 authentication process.It is utilized for the different type of validation of remote users. CHAP has 3 way handshaking procedure. It involves a three-way exchange of a shared secret. CHAP uses MD5 algorithm to calculate a value known by the remote device in addition to the authentication system.with this authentication method,user ID & password are always sent in encrypted form.

3. TPA

Third party auditor (TPA) for public auditing. TPA offers its auditing service with more powerful computation and communication abilities[2].

4. MD 5 Hash

The only way to verify a correct password is by comparing the user provided (hashed using MD5) with the hashed password in the database. The secret string of letters used in the hashing process is known as a Key.

5. Shamir's Secret Sharing

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 server we validate the customer utilizing Shamir's secret sharing Shamir's Secret Sharing is used to secure a secret in a distributed way, most often to secure other encryption keys. The secret is split into multiple parts, called shares. These shares are used to reconstruct the original secret. To unlock the secret via Shamir's secret sharing, you need a minimum amount of shares. This is called the threshold, and is used to represent the minimum amount of shares needed to unlock the secret.

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

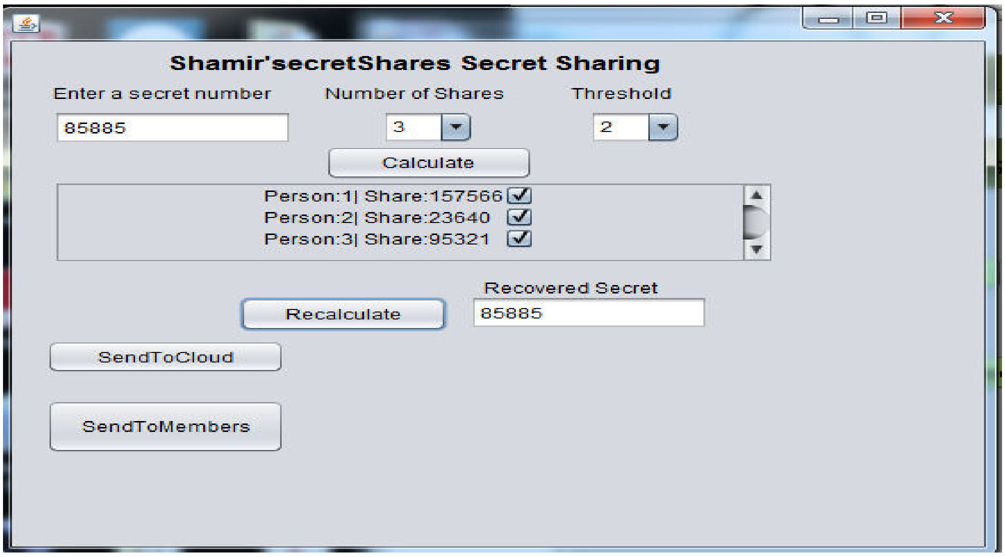
Share
Share is a piece of secret. Secret is divided into pieces and each piece is called share.
It is computed from given secret. In order to recover the secret, you need to get certain numbers of shares.

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.

V. METHODOLOGY

In Proposed system md5 hash code is used for encryption. When user upload file on cloud using first hash code and if attacker makes changes in file i.e. edit in file or add content in file then hash code also changes. And length of file is also changes due to this hash code difference arises . When TPA match the mac id then there will be difference in hash code.

Step 1. User/owner encrypted file using AES algorithm with unique Mac ID
Step 2. User send encrypted file to cloud & TPA
Step 3. User divide key into shares (key is shared between selected clients/candidates) using secret Shamir algorithm
Step 4. After key is shared , request has been send to all shares
Step 5. When shares/clients approved request then verification key send by cloud through Email ID of each share & Alphanumeric file password is send on owners Email id
Step 6. TPA verify the file for download request. When user request a file for downloading, the key access request is additionally sent to all or any members to whom the divided Shamir's secret key's 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.
Step 7. If TPA is approved for user's request for purpose of file download ,the file is available at users/owners account. While downloading file First user put alphanumeric password which is send by CSP on email id, The user selects the downloaded encrypted file and decrypts it, after decryption the client will able to view the original uploaded data.



Shamir'secretShares Secret Sharing

Enter a secret number: 85885

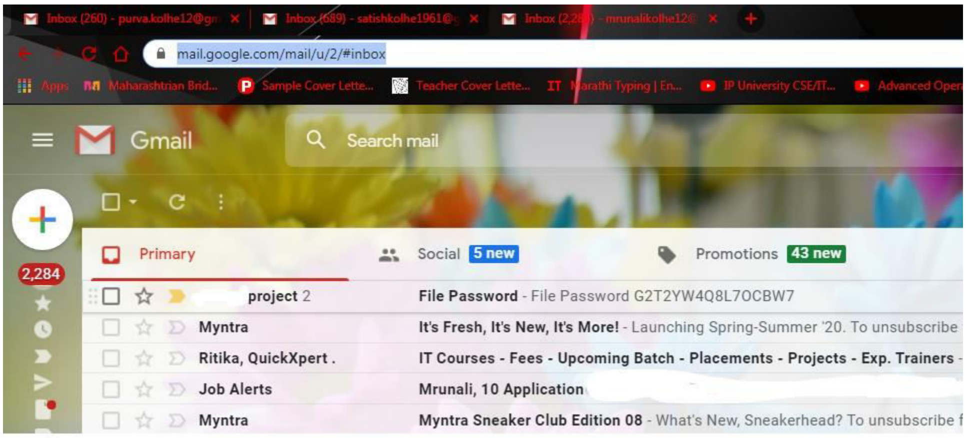
Number of Shares: 3

Threshold: 2

Person:1| Share:157566 ☑
Person:2| Share:23640 ☑
Person:3| Share:95321 ☑

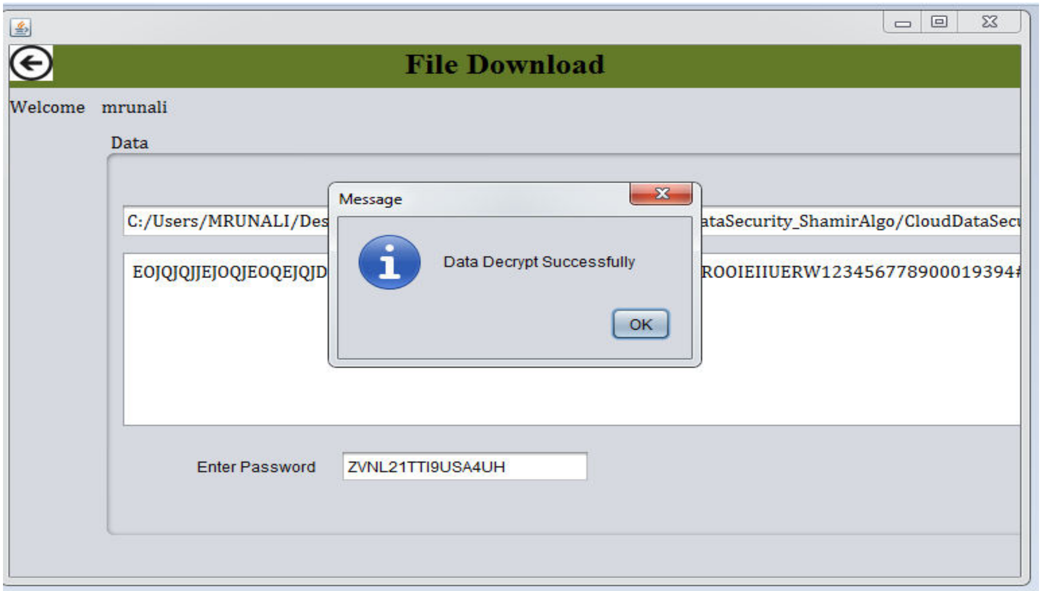
Recovered Secret: 85885

Fig 2. Shamir secret sharing algorithm



project 2	**File Password** - File Password G2T2YW4Q8L7OCBW7
Myntra	**It's Fresh, It's New, It's More!** - Launching Spring-Summer '20. To unsubscribe
Ritika, QuickXpert .	**IT Courses - Fees - Upcoming Batch - Placements - Projects - Exp. Trainers** -
Job Alerts	**Mrunali, 10 Application**
Myntra	**Myntra Sneaker Club Edition 08** - What's New, Sneakerhead? To unsubscribe f

Fig 3. File password sent on Owner’s Email Id(without this password ,file can not decrypted)



Welcome mrunali

C:/Users/MRUNALI/Des ... ataSecurity_ShamirAlgo/CloudDataSecu

EOJQJQJJEJOQJEOQEJQJD ... ROOIEIIUERW123456778900019394#

Data Decrypt Successfully

Enter Password ZVNL21TTI9USA4UH

Fig 4. Decryption of file

VI. RESULT ANALYSIS

The performance study and comparison through a proposed framework Using AES Encryption and Shamir's Secret Sharing for Secure Cloud gives better result that includes - more secure, less file access time and better output which leads to providing a better and secure cloud service.

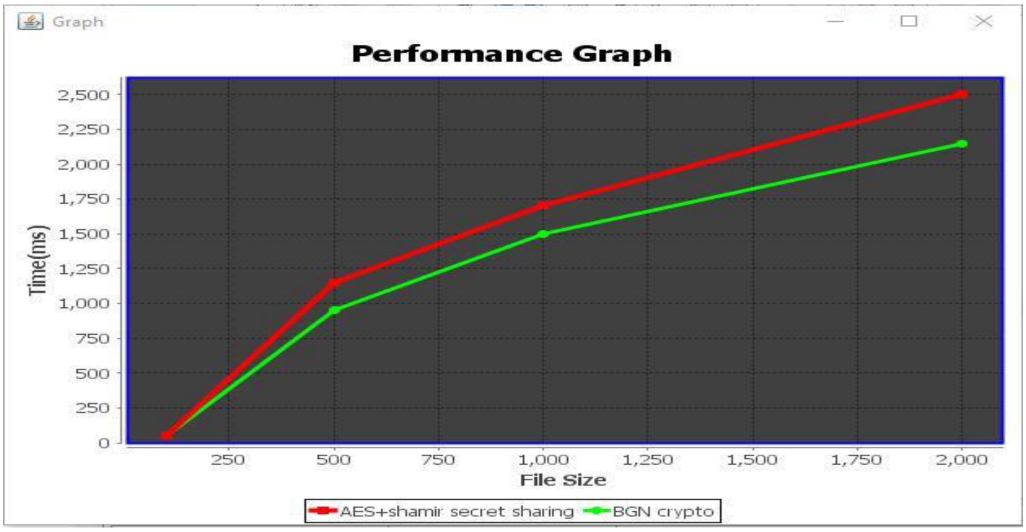


Fig 5. Performance Graph between Existing System and Proposed System

This performance graph indicate that the proposed framework utilizing AES encryption, TPA and Secret Shamir's key sharing Algorithm can perform superior than existing approach in framework of privacy preserving.

VII. CONCLUSION

In cloud computing data storage security and integrity is that the main issue to be resolved. This paper proposed a structure which is capable of providing secure and trusted mechanism for cloud data security and data integrity. By utilizing this proposed framework one are often assured that their outsourced data won't be vulnerable while the cloud auditing process. Using Shamir's secret sharing to authorize customers, Hash Key for data integrity check and AES Algorithm for encoding this framework can decrease the computational cost of storage service providers and to make sure the integrity of the Cloud User's data stored within the cloud data centre.

REFERENCES

1.Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE" Privacy-Preserving Public Auditing for Secure Cloud Storage"

2.Ankush R. Nistane1, Shubhangi Sapkal2, Dr. R. R. Deshmukh3," Privacy Preserving Public Auditing and Data Integrity for Secure Cloud Storage Using Third Party Auditor" IJAEMSVol-2, Issue-2, Feb- 2016

3.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),

4. L. Malina, J. Hajny, P. Dzurenda and V. Zeman," Privacy-preserving security solution for cloud services" Journal of Applied Research and Technology, Vol. 13, February 2015

5.Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data ,Ako Muhamad Abdullah ,MSc Computer Science –UK ,PhD Student in Computer Science Student No. 16600094 , Cryptography and Network Security Publication Date: June 16, 2017

6.Privacy-Preserving Selective Aggregation of Online User Behavior Data, Jianwei Qian, Fudong Qiu, Student Member, IEEE, Fan Wu, Member, IEEE, Na Ruan, Member, IEEE, Guihai Chen, Member, IEEE, and Shaojie Tang, Member, IEEE IEEE Transactions on Computers (Volume: PP, Issue: 99),28 July 2016

7. SECURITY AND PRIVACY OF SENSITIVE DATA IN CLOUD COMPUTING: A SURVEY OF RECENT DEVELOPMENTS, Ali Gholami and Erwin Laure HPCViz Dept., KTH- Royal Institute of Technology, Stockholm, Sweden, pp. 131–150, 2015. © CS & IT-CSCP 2015, DOI : 10.5121/csit.2015.51611

8. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Wenjing Lou, Senior Member, IEEE, and Jin Li

9.Privacy Preserving Issues and their Solutions in Cloud Computing: A Survey Pooja HP 1, MTech(CSE), BMSCE, Bangalore, India. , Nagarathna N 2 Prof. Dept. of CSE, BMSCE, Bangalore,India. IJCSIT Vol. 6 (2) , 2015, 1588-1592

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details

www.ijircce.com