IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMPLEMENTATION OF SECURE CLOUD WITH PRIVACY PRESERVING PUBLIC AUDITING.

[1]Revti R. Adel, [2]Dr. V.M. Deshmukh.

[1]Final year M.E., [2]Associate Professor, Department of Computer Science and Engineering, PRMIT&R.
[1]Computer Science and Engineering,
[1]Student, Amravati, India

Abstract: Computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. By using cloud storage, users can access applications, services, software whenever they require over the internet. Users can put their data remotely to cloud storage and get the benefit of on-demand cloud services and application from the resources. The cloud must ensure data integrity and security of data of the user. The issue about cloud storage is integrity and privacy of data of the user. To maintain 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 system also supports data dynamics. The work that has been done in this line lacks data dynamics and true public audit ability. The auditing task monitors data modifications, insertions and deletions. The implement system is capable of supporting public audit ability, 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. Markel Hash Tree is used to improve block level authentication.

Keywords **- Cloud Storage, Data Dynamics, Public Auditing, Privacy Preserving**

I. INTRODUCTION

Cloud Computing is attaining more and more generosity in both the intellectual and industrial community. It becomes an imitation for recognizing everywhere, well-located, on-demand network connection for all the configurable computing resources (i.e., networks, services, servers, applications). 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 the 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. So the basic motivation behind this is

A. Motivation

- To overkill this issue, public auditing process is introduced 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 implement 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 implement system is capable of supporting public auditability, data dynamics and Multiple TPA are used for the auditing process.

B. Objective

The system aims to achieve the following objectives:

1. **Public Auditing:** The public verifiers (TPA) are capable to publicly certifying the integrity of the data to be shared away from retrieving the whole data within the cloud.
2. **Correctness:** The public verifiers (TPA) are adept at correctly verifying the integrity of data to be shared.
3. **Unforgeability*:*** Only the user within the group can have authority to generate valid verification (i.e., signatures) on shared data.
4. **Identity Privacy*:*** The public verifier (TPA) cannot distinguish the identity of the user on each block which shared data during the process of auditing.

Mainly, users can abandon the maintenance of IT services to cloud service providers (CSP), who are apt in providing knowledge and maintaining the large amount of IT resources. Cloud computing causes many new security issues and challenges on assuring the integrity and privacy of users data in the cloud. To entice these issues, our work uses the concept of secret key which is based on symmetric key cryptography, in which it allows the TPA to execute the auditing without exacting the local copy of the user's stored data and hence sharply analyze the transmission and reckoning overhead as related to the straightforward data auditing approaches. So to accommodate the encryption with examining, our protocol ensures that during the efficient auditing process, the TPA could not get any information about the data context stored within the cloud server. Our work is one of the first few ones in this field to deliberate in storage security of distributed data storage in Cloud Computing.

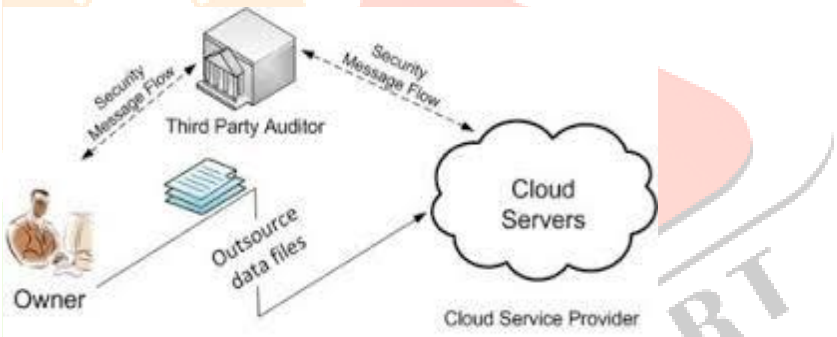

Fig. 1 : Third Party Auditor

The Fig 1. shows how third party auditor (TPA) it consist three different entities: the cloud user, the cloud server (CS) and the third party auditor (TPA) As shown in fig. 1. The cloud user is the one who has a large number of data files that are stored in the cloud; the cloud server is the one who provides the data storage service like resources, software to the user. The cloud server is managed by a cloud service provider; the third- party auditor is the one who has a belief to access the cloud storage service for the benefit of the user whenever the user requests for data access. The TPA has capabilities and competence that the user does not have. They can also interact with a cloud server to access the stored data for different purposes in a different style. Every time it is not possible for the user to check the data which is stored on a cloud server that arrives online, burden to the user. So that's why to reduce online burden and maintain the integrity of cloud users may resort to TPA.

II. SYSTEM ANALYSIS/DESIGN

A. Analysis

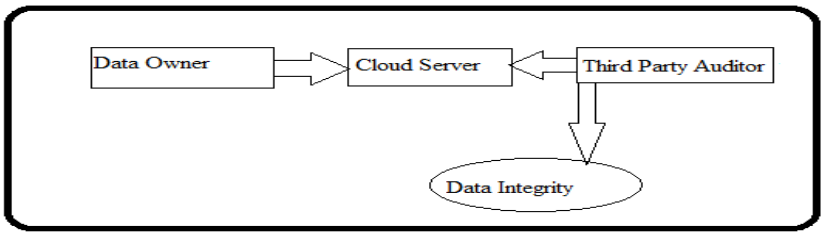

Fig. 2 : Cloud Server Storage

The system network for cloud data storage is illustrated in Fig 2. Three different network entities can be identified as follows.

1.Data Owner (Client) An entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations.

2.Cloud Storage Server (CSS) An entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the client's data.

3.Trusted (Third) Party Auditor (TPA) An entity which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request. The data owner registered with a cloud service provider and stores their data in a cloud server by using the private key. To check the integrity of data stored in a cloud server, the data owner sends a request to the Third Party Auditor (TPA). The TPA audit the files stored in the cloud server by using top hash value which it gets from the data owner.

1. Problem Definition

To provide the main important thing, data integrity and security to the cloud, public auditing is given. The scheme performs the public auditing in which hashing technique is used as well as the scheme performs data dynamic operation like insert, update, delete in a block-wise manner. When there are some problems like users load, system crash, system failure, then the scheme uses multiple TPA. TPA do the auditing process in which if there is a failure of one TPA, another TPA does the auditing process by taking backup of the first TPA.

2. Requirement Analysis

1. Operating System : Windows 7, 8, 10
2. Languages Used: PHP,HTML
3. Database Used : Mysql
4. Library : jQuery

B. Design

There is a need to develop an effective public auditing protocol which overcomes the limitation of the existing auditing scheme. The system is developed to verify the correctness of cloud data by TPA, periodically or on demand without retrieving the entire data or without introducing additional online burden to the cloud users and cloud servers. It assures that no data content is leaked to TPA during the auditing process. It maintains storage correctness of data, integrity and confidentiality of stored data.

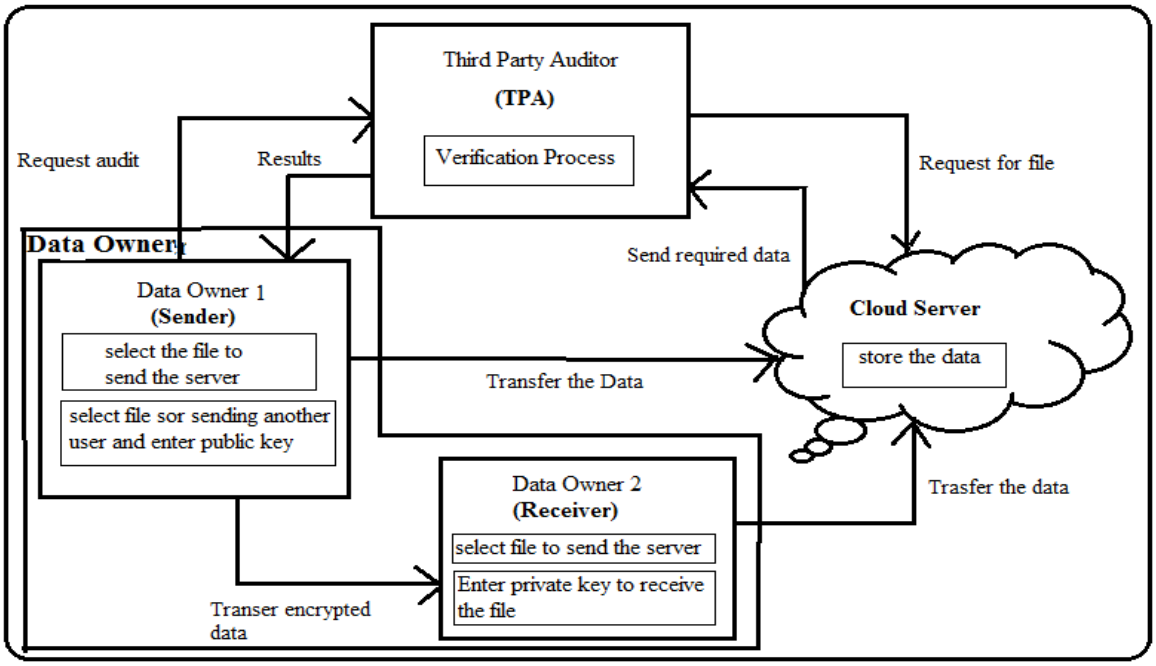

Fig. 3 : Auditing scheme Architecture

The design scheme consists of three basic entities; they are

1. **Data owner:** Data owner is an important part of our system. It performs most of the responsibility related to the data. In the auditing scheme, the data owner first performs login and registration with a cloud server and TPA. The new user has to first register itself by filling the registration form and be an active member of the system. A message for successful registration will be provided. If a user is already a member of the system, then he or she can perform the login process. If the user name and password exist in the database, then they will be able to login successfully for being valid users, or else they will receive an error message. Once successfully login, the data owner will select the file he or she wants to store on the cloud server. The file selected by him/her is then transferred to the cloud server. If one user wants to send a file to another user. To provide security to the communication, we use RSA and Base 64 encryption algorithm. First, the sender encrypts the file by entering the public key and then send the file and then the receiver receives it by entering the private key to decrypt the file and receiving it.

2. **Cloud Server Storage:** Cloud server stores the data which is transferred by the data owner and sends the requested data to the third party auditor.

3. **TPA:** In the implement scheme, to perform the task of data auditing, a TPA is been used for this purpose. TPA performs data auditing either periodically or on demand by the client. On receiving the auditing request from a user or data owner, the TPA starts its auditing process. Later it compares the two signatures in the verification process. If it matches, it means the integrity of data is maintained and otherwise not maintained. This means that data has not been tampered or changed. The results for the same are provided to the data owner by the TPA.

C. Detail Designed

Algorithm

To provide the security to the communication between the data owners, this dissertation used RSA algorithm and base 64 encryption algorithm.

RSA Algorithm

RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly

described the algorithm in 1977. The RSA algorithm is an asymmetric cryptography algorithm; this means it uses a public key and a private key (i.e., two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone. The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman. The following illustration highlights how asymmetric cryptography works:

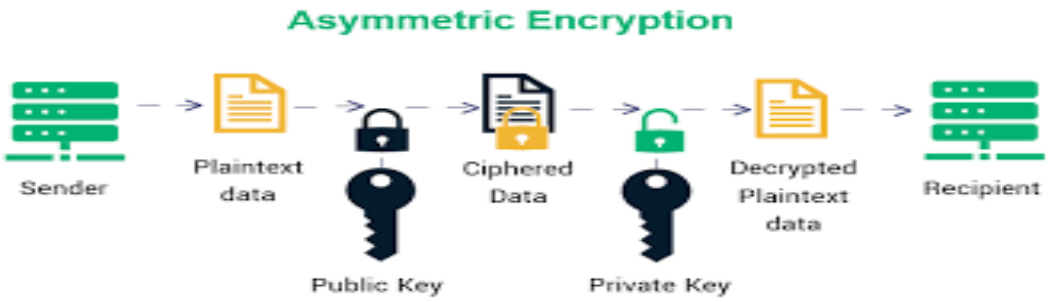

Fig. 4 : Asymmetric Encryption

How it works

The RSA algorithm ensures that the keys, in the above illustration, are as secure as possible. The following steps highlight how it works:

1. Generating the keys

1. Select two large prime numbers, X and Y. The prime numbers need to be large so that they will be difficult for someone to figure out.
2. Calculate n = X * Y.
3. Calculate the totient function; $\phi(n)=(X-1)(Y-1)$.
4. Select an integer e, such that e is co-prime to $\phi(n)$ and $1<e<\phi(n)$. The pair of numbers (n, e) makes up the public key.

2. Encryption

Given a plaintext P, represented as a number, the cipher text C is calculated as:

C = P^{e}mod n.

3. Decryption

Using the private key (n, d) the plaintext can be found using:

P = C^{d} mod n

Base 64 Algorithm

The Base64 algorithm is designed to encode any binary data, a stream of bytes, into a stream of 64-printable characters. In PHP we use base64_encode() function which is an inbuilt function in PHP which is used to encode data with MIME base64. MIME (Multipurpose Internet Mail Extensions) base64 is used to encode the string in base64. The base64_encoded data takes 33% more space than the original data.

Syntax:

string base64_encode($data)

The Base64 encoding process is to:

- Divide the input bytes stream into blocks of 3 bytes.
- Divide 24 bits of each 3-byte block into 4 groups of 6 bits.
- Map each group of 6 bits to 1 printable character, based on the 6-bit value using the Base64 character set map.
- If the last 3-byte block has only 1 byte of input data, pad 2 bytes of zero (\x0000). After encoding it as a normal block, override the last 2 characters with 2 equal signs (==), so the decoding process knows 2 bytes of zero were padded.
- If the last 3-byte block has only 2 bytes of input data, pad 1 byte of zero (\x00). After encoding it as a normal block, override the last 1 character with 1 equal signs (=), so the decoding process knows 1 byte of zero was padded.
- Carriage return (\r) and new line (\n) are inserted into the output character stream. They will be ignored by the decoding process.

D. Flowchart

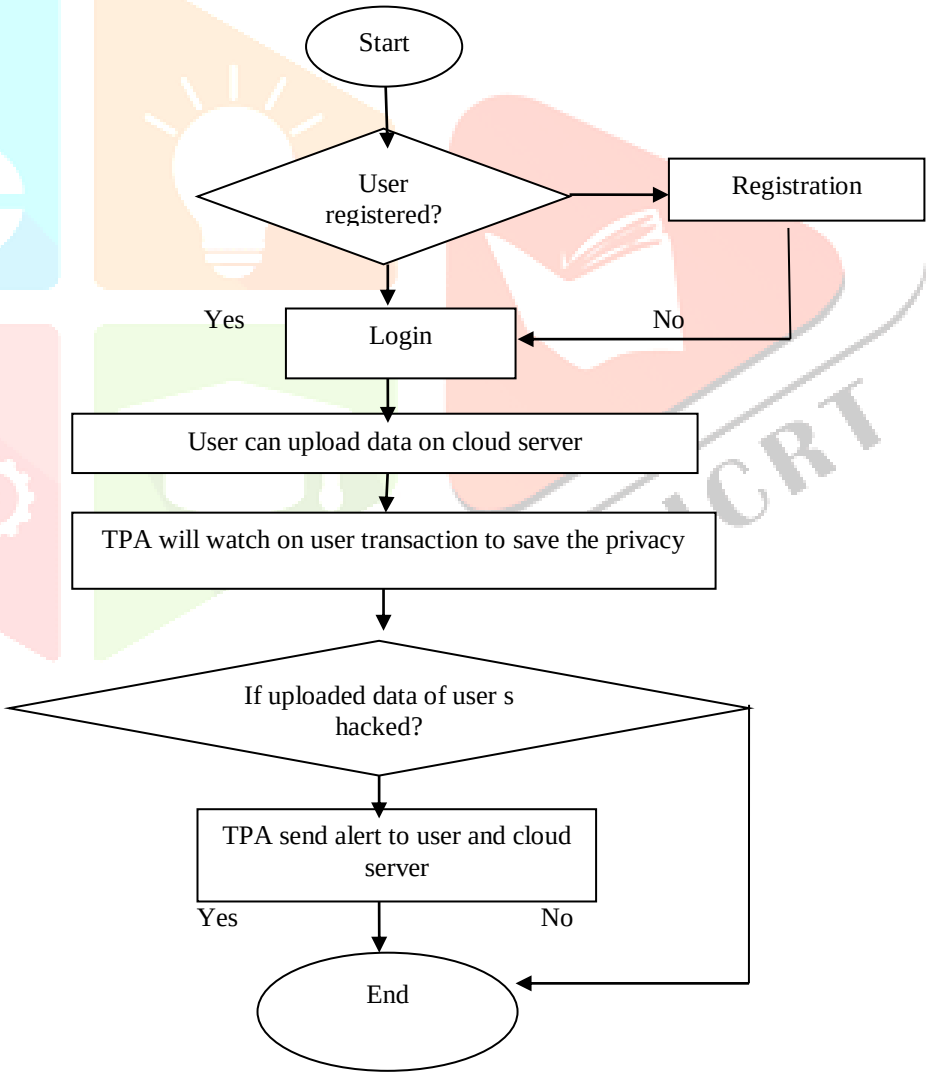

Fig. 5 : Flow Chart

III. IMPLEMENTATION DETAILS

The system is implemented by using :

1. **HTML**
2. **CSS**
3. **JAVASCRIPT**
4. **BOOTSTRAP**
5. **PHP**
6. **XAMPP**

A. System Execution Details

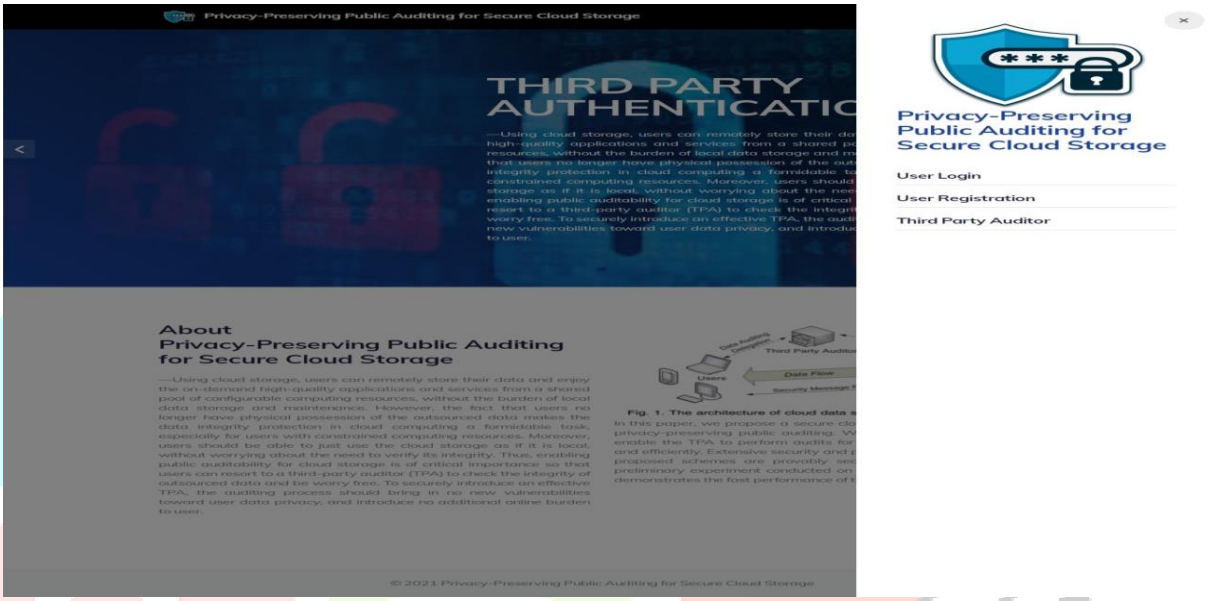

Fig. 6 : Application for privacy preserving public auditing for secure cloud storage system

The above fig. 6 shows home page of privacy preserving public auditing for secure cloud storage system. When user clicks on the upper right side of the three horizontal line icon on the home page, the main links of the working system are open. These links are user login, user registration and third party auditor. If there is a new user to the system, first of all the new user has to register themselves. By clicking on the user registration on the main link, this registration form will be open. When a user enters the system, then they have to authenticate their self. Once the registration of the user is completed, users are allowed to authenticate their selves. The following fig. 7 shows public and private key generation. When one user wants to send any message or any file to another user. This system provides security to the communication by using RSA and Base 64 encryption algorithm. When one user wants to communicate with another user, at that time dynamic public and private keys are generated.

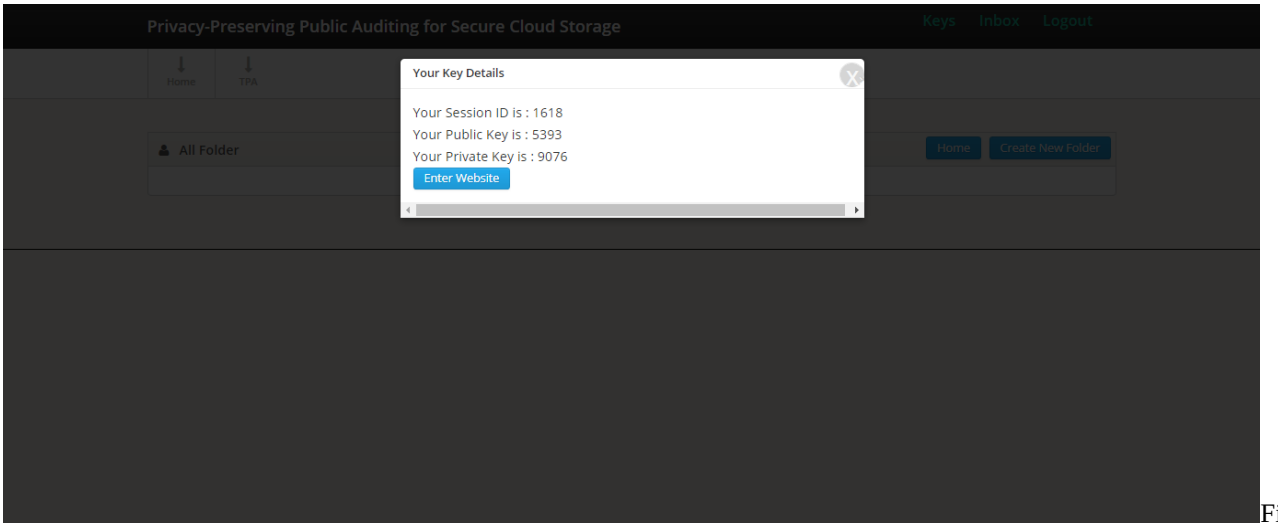

Fig. 7 : Public and Private Key Generation.

When a user wants to create a new folder, then by clicking on creating a new folder, a new folder is created. Upload the file by entering the private key page. When the user wants to upload the file in the created folder. They have to first enter the private key to enter the file.

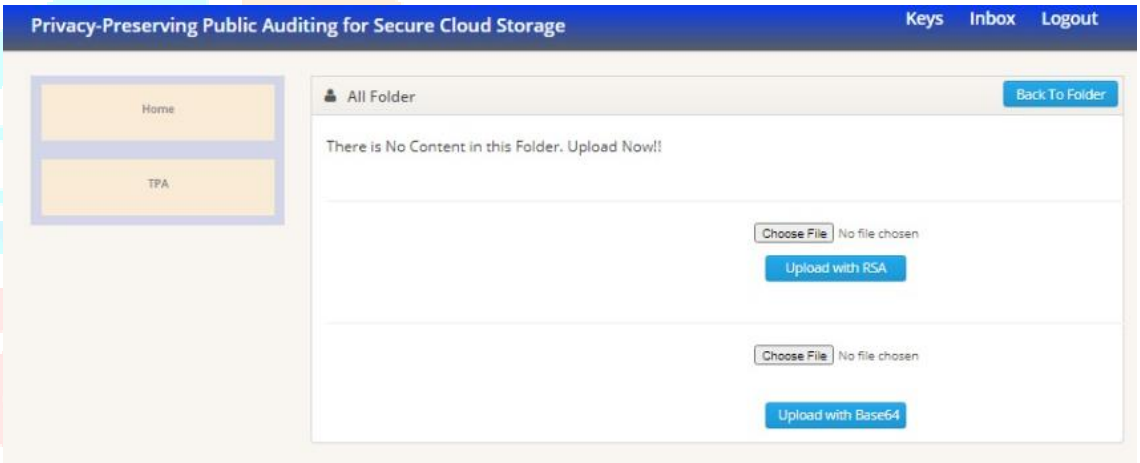

Fig. 8 : Upload File

The above fig. 8 shows uploading a file page. Here users are allowed to upload a file in two ways, by using RSA and by using base 64. Users are allowed to send the file to another user with a message. The following fig. 9 shows encrypted data. While uploading the data by the data owner, the data is encrypted by using RSA algorithm & Base 64 encode algorithm. And it looks like as shown in Figure.

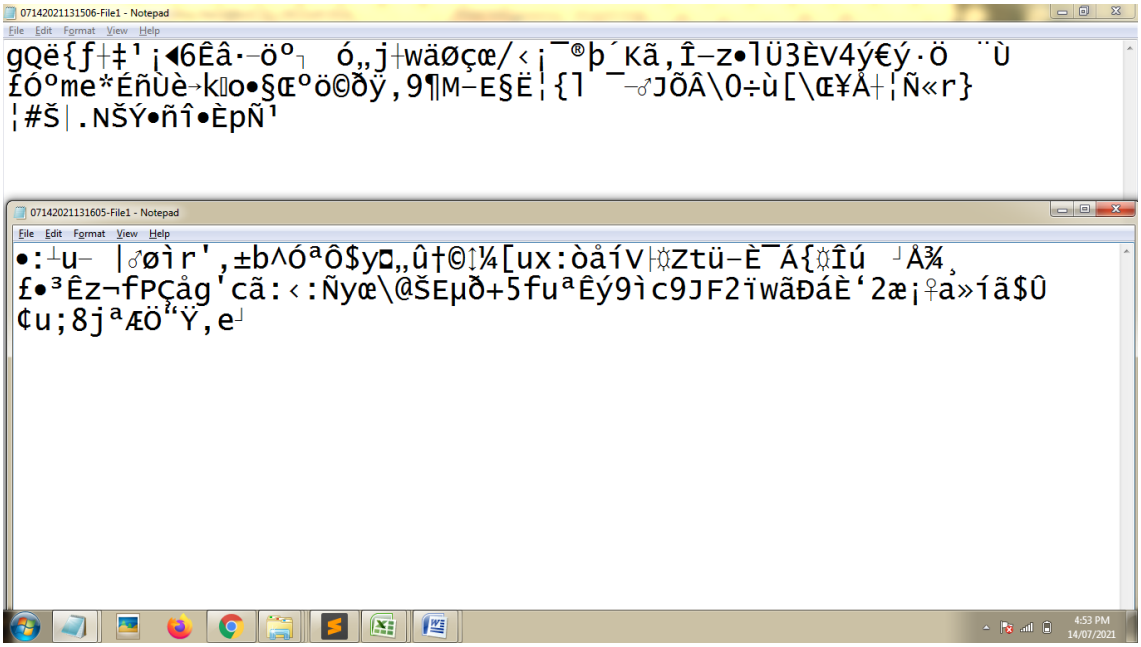

Fig . 9 : Encrypted data using RSA and Base 64 Encode Algorithm.

The data owner or receiver are allowed to see the received files. You can download the received files by clicking on the download file. When the receiver wants to download the file, the user must enter the public key first. Once a public is entered by a user, then users are allowed to see the file with a message by clicking on it. Also, the message and file get decrypted.

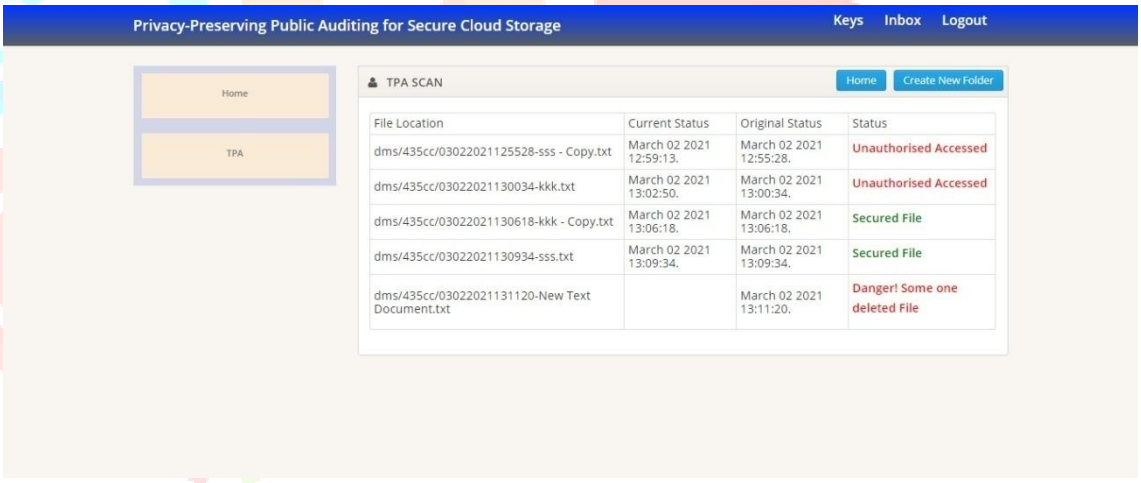

Fig. 10 : TPA Scan

The above Fig. 10 shows TPA scan page. The most important feature in this dissertation is TPA (Third Party Auditor). TPA SCAN each and every file in the user directory. Keep and watch every file, its source file details and current file status. If any mismatched found means there is an Unauthorized Accessed to the file. If someone an intruder deleted a file from the server, then TPA shows a message “Danger!". Someone deleted File.” If the file is secure, then show the message “Secured File.”

B. Result Analysis

File Name	File size	Uploading time by RSA	Uploading time by Base 64
File 1	5.52 kb	17.8 sec	16.1 sec
File 2	7.3 kb	30.8 sec	16.3 sec

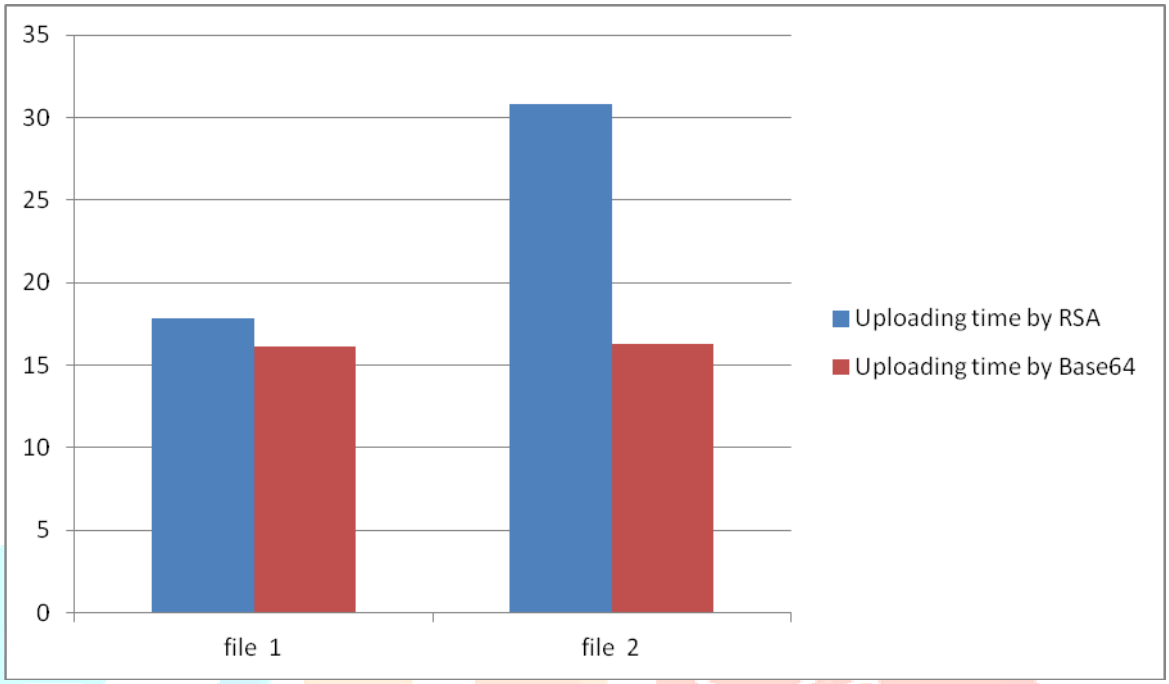

Fig. 11 : Bar Graph

The bar graph shows the performance of the RSA algorithm and the base 64 algorithm which are implemented in the working system of this report. The performances of both the algorithms are in terms of time required to upload and encrypt the file. To compare the performance of both algorithms, we upload two files for encryption by two ways. According to the above result, RSA takes more time than Base 64.

IV. Conclusions

A secure and efficient privacy preserving public auditing scheme is been implemented. It achieves privacy preserving and public auditing for cloud by using a TPA (Third Party Auditor), which does the auditing without retrieving the data copy, hence privacy is preserved. The data stored in the encrypted format in the cloud storage, thus maintaining the confidentiality of data. The data integrity is verified by. It only checks whether the stored data is tampered or not and informs about it to the user. An attempt is made to overcome the limitations of the existing auditing scheme.

V. Acknowledgment

It is a matter of great pleasure by getting the opportunity of highlighting a fraction of knowledge we acquired during our technical education through these assignments. This would not be possible without the guidance and help of many people. This is the only page where we have an opportunity of expressing our emotion and gratitude from the care of my heart. These assignments would not have been successful without enlightened ideas timely suggestions and our most respected guide. Dr. V. M. Deshmukh without her best guidance this would have been an impossible task to complete. Being on the same line, we all express our deep sense of gratitude to our heads of the Department Dr. G. R. Bamnote sir for this most valuable guidance provided by him. Last but not least, we would like to express our thankfulness to the teaching and non-teaching staff, our friends and all my well - wishers.

REFERENCES

[1] https://en.wikipedia.org/wiki/cloud_computing

[2] C. Wang, Q. Wang, K. Ren, a n d W. Lou, "Privacy- Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM "10, Mar. 2010.

[3] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloud computing/index.html, June 2009.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS "07), pp. 598-609, 2007.

[5] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Int"l Conf. Security and Privacy in Comm. Networks (SecureComm "08), pp. 1-10, 2008.

[6]. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Service Computing, vol. 5, no. 2, 220-232, Apr.-June 2012.

[7] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS "07), pp. 584-597, Oct. 2007.

[8] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from The Weil Pairing," J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.

[9] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. 16th ACM Conf.Computer and Comm. Security (CCS "09), 2009.

[10] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Storage Systems," in Proc. ACM Cloud Computing Security Workshop (CCSW), 2010, pp.31– 42.

[11] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems(HotOS "07), pp. 1-6, 2007.

[12] https://en.wikipedia.org/wiki/Merkle_tree.

[13] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS "07), pp. 598-609, 2007.

[14] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Int"l Conf. Security and Privacy in Comm. Networks (SecureComm "08), pp. 1-10, 2008.

[15] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Service Computing, vol. 5, no. 2, 220-232, Apr.-June 2012.

[16] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS "07), pp. 584-597, Oct. 2007.

[17] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from The Weil Pairing," J. Cryptology, vol. 17, no. 4, pp. 297 - 319, 2004.

[18] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS "09), 2009.

[19] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems(HotOS "07), pp. 1-6, 2007.

[20] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Storage Systems," in Proc. ACM Cloud Computing Security Workshop (CCSW), 2010, pp.31– 42.

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

[22] M. Franz, P. Williams, B. Carbunar, S. Katzenbeisser, and R. Sion, "Oblivious Outsourced Storage with Delegation," in Proc. Financial Cryptography and Data Security Conference (FC), 2011, pp. 127– 140.