

NEW APPROACH OF TPA BASED DATA ACCESS MODEL

¹Ashish, Bhardwaj, ²Surendra, Yadav

Abstract

Data Access and storage are the basic needs for any organization and they are a part of any organization routine activity. When performing data access, the main concern is regarding the ease of access of data and transfer of data with the proper security for that data. Data access distinguishes the roles & the responsibilities between the abilities of administrators & that of end users while accessing the repository or the stored data. This paper presents TPA based security model which performs data sharing through encrypted data chunks. This model is not only effective in terms of the data transfers but also is more secure than the existing models.

Keywords: TPA Based Security, Cloud Storage, Data Access, Data Storage

I. Introduction

Cloud storage is a cloud processing model that stores data on the Internet through a cloud-computing supplier who oversees and works data storage as a help. The data is delivered on demand within the nick of time limit and costs and wipes out purchasing and dealing with your own data storage foundation. This gives you deftness, worldwide scale and sturdiness, with "whenever, anyplace" data access. With cloud storage, there is no equipment to buy, storage to arrange, or capital being utilized for "sometime in the not so distant future" situations.

You can include or expel limit demand, rapidly change execution and maintenance qualities, and just compensate for the storage that you really use. With the decrease in time accessed, data can even be naturally moved to bring down cost levels as per auditable guidelines, driving economies of scale. [1]

At the point when advancement groups are prepared to execute, framework should never back them off. Cloud storage permits IT to rapidly convey the specific measure of storage required right when it is required. This permits IT to concentrate on taking care of complex application issues as opposed to overseeing storage systems. [1]

Cloud storage is characterized as "the storage of data online in the cloud," wherein an organization's data is put away in and accessible from multiple layer and associated assets that together form a cloud. Cloud storage can give the advantages of better accessibility and unwavering quality, quick sending, solid security for data reinforcement, chronicled and fail recovery purposes; and significantly lower large storage costs because of not buying, overseeing and keeping up costly equipment. There are numerous advantages to utilizing cloud storage but on the flip side, cloud storage has the potential for security and consistence worries that are not related with customary storage systems. [2]

¹ School of Computer Science & System Studies, Career Point University, Alaniya, Jhalawar Road, Kota-325003, Rajasthan, India

² School of Computer Science & System Studies, Career Point University, Alaniya, Jhalawar Road, Kota-325003, Rajasthan, India

II. Literature Review

Bin Feng et. al 2016, Authors of this paper constructed an auditing system which will be utilized for the cloud storage systems and which thus led to the usage of a proficient and security protecting auditing convention. The authors stretched out the auditing convention to help dynamic data tasks which was seen as proficient in the random prophet model. The conventions likewise bolster the bidirectional authentication and utilizes a better burden circulation system which helps in decreasing the computational overhead of the customer. But we have found a few gaps in the paper which led to the premise of our proposed approach:

- provide data privacy in Amazon based cloud foundation storage administrations
- Verify the authentication of evaluating records and guarding against attacks and byzantine faults.
- Develop a Novel Remote Integrity Verification Technique for checking the cloud user.
- execute the Novel Data Block Integrity Verification model for giving the storage security
- Develop a Novel Access Control Structure based policy Generation Technique for the confined access of the stored data blocks by the cloud users.

M. A. Mohammed et. al 2016, Cloud specialist co-op module is to process data proprietor demand for storing data documents and application and give cloud users' log details to data proprietor for audit reason. This paper focusses the issue of system based on data responsibility and preliminary of the real handling of the users' data in the cloud is to be done. The idea which is proposed by the authors is that the data can be completely traceable by the proprietor and the proprietors can catch up the administration concurrences based on the different sorts of things like access, use control and management.

O. Heinisuo, et. Al 2019, In this paper, the authors work with the likelihood to utilize cell phones as the decentralized record sharing stage without utilizing any of the focal specialists. Authors accomplished this by the usage of a framework which they named Asterism, which is a distributed record sharing versatile application that is based on the Inter-Planetary File System. They approved the outcomes by conveying and then estimating up the application network use and force utilization by analyzing that on multiple gadgets. The investigation results of the created structure show that cell phones can be utilized to actualize the overall dispersed document sharing network.

III. Proposed Approach

This segment is compares to make sure of record partaking in the cloud-based condition with the best possible approval of the user.

In the period of the approval of the user, we are likewise utilizing the TPA which is a third-party authenticator.

So, the entire procedure of sharing incorporates,

- User Authentication
- User File Encryption
- Server Retrieval

User Authentication Algorithm

This segment deals with the user approval for accessing the cloud administrations for the accessing or the recovery of the data.

Step 1: First allotted the TPA for the approval of the users.

Step 2: Access the rundown of the legitimate users for the administration to approve the user requesting the administration of the document access or record storage.

Step 3: In request to additionally twofold approve the character of the user, an OTP containing six random digits together with the 3 digits extracted from the user id.

Along these lines, the general configuration of the OTP will resemble,

R1R2R3R4R5R6X1X2X3

Where,

- R1,R2,R3,R4,R5,R6 are the random numbers ranging between 0 to 9, both inclusive.
- X1X2X3 are the initial three digits extracted from the user id of the user requesting for the cloud administration.

Step 4: The OTP produced will be sent to the user requesting by utilizing the enlisted email id just as to the unique identification number

Step 5: User at that point enters the OTP and sends the OTP back for the approval by the TPA.

Step 6: If approved at that point, proceed for accessing the cloud administrations Else Goto Step 7.

Step 7: Stop.

User File Encryption and storage

So as to approve the uprightness of the record, the idea we put forth is that it's creates an MD5 hash of the document sent on the sender end and at the receiver end, the pieces are joined. The MD5 hash is again produced to crosscheck that both hashes are same and if both the hash are same, the record will be treated as valid.

Step 1: Read the record user name

Step 2: Select the segment from the data stacked which decides the bases for the bunching.

Step 3: Create the Clusters of Special Characters, Lower case letters in order, Upper case letters in order, Numbers and score based on the size of the quantity of components in the bunches.

Step 4: The Clusters are then divided into groups based on the size of the components in the groups.

Step 5: Every time, a random bunch is chosen from each group.

Step 6: Then, a random password is created and utilized for encryption with the AES algorithm

Step 7: Store the details of the randomly chosen group (combine with bunch ID with the arrangement number) and key on the cloud server with the interested record id.

Step 8: Generate Hash for the first document using the MD5 algorithm.

Step 9: Also store the document related hash with a unique record id on the cloud server.

Step 10: Stop

File Retrieval

This area is utilized by the user requesting the access for the document put away on the cloud server.

Step 1: Read the UserName (The procedure of the retrieval will start simply after the user approval or authentication is finished).

Step 2: File ID mentioned, User needs to give the MD5 hash of the record mentioned.

Step 3: If server accesses the record utilizing the File ID and accesses the MD5 hash of the document, Goto Step 4

Step 4: If MD5 Hash coordinates then Goto Step 5 Else Goto Step 14.

Step 5: Access the Cluster of the File ID.

Step 6: Prompt for the key based on the Cluster ID.

Step 7: If Key is approved then Goto Step 8 Else Goto Step 14

Step 8: Decrypt the bunch and store back the group..

Step 10: Rearrange all bunches and join the document.

Step 11: Calculate the MD5 hash of the resultant record. [Hash is created here for trustworthiness check]

Step 12: If same then Goto Step 13 Else Goto Step 14

Step 13: Grant access to the document and transfer the record.

Step 14: Stop.

IV. Implementation

The implementation is done using software Visual Studio and SQL Express Edition for database.

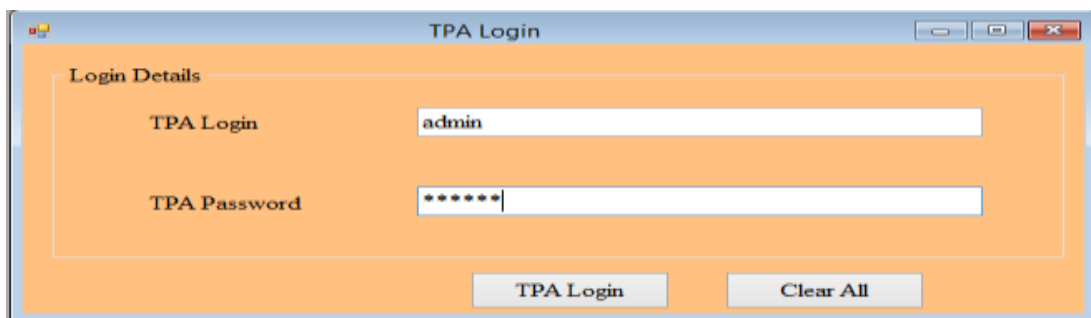


Figure 1: TPA Login

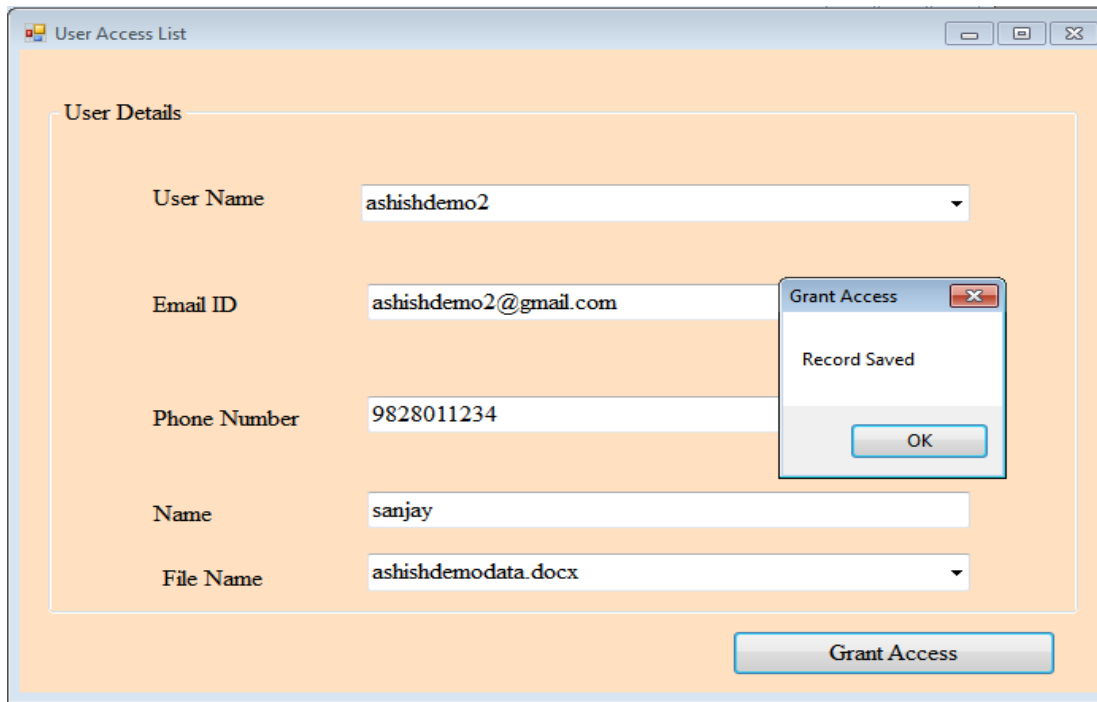


Figure 2: Access Granting Form

The implementation is based on using the TPA based Security model, where the User access list is maintained by the TPA.

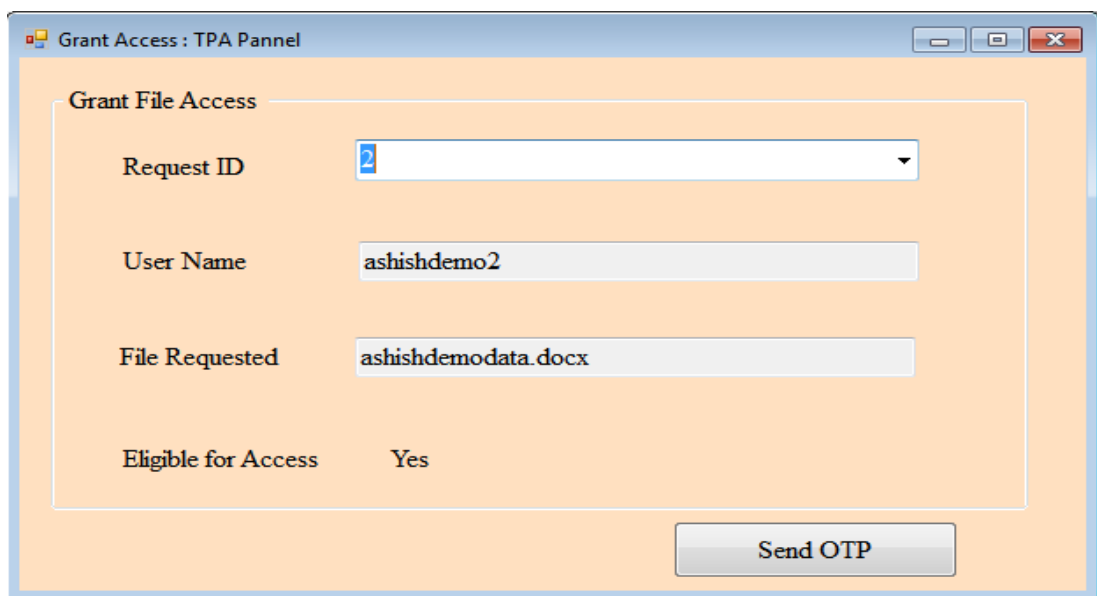


Figure 3: User Validation Form

The TPA will first check whether the user is eligible to access and then an OTP is sent to the user in order to access the file.

The general format of the OTP will look like,

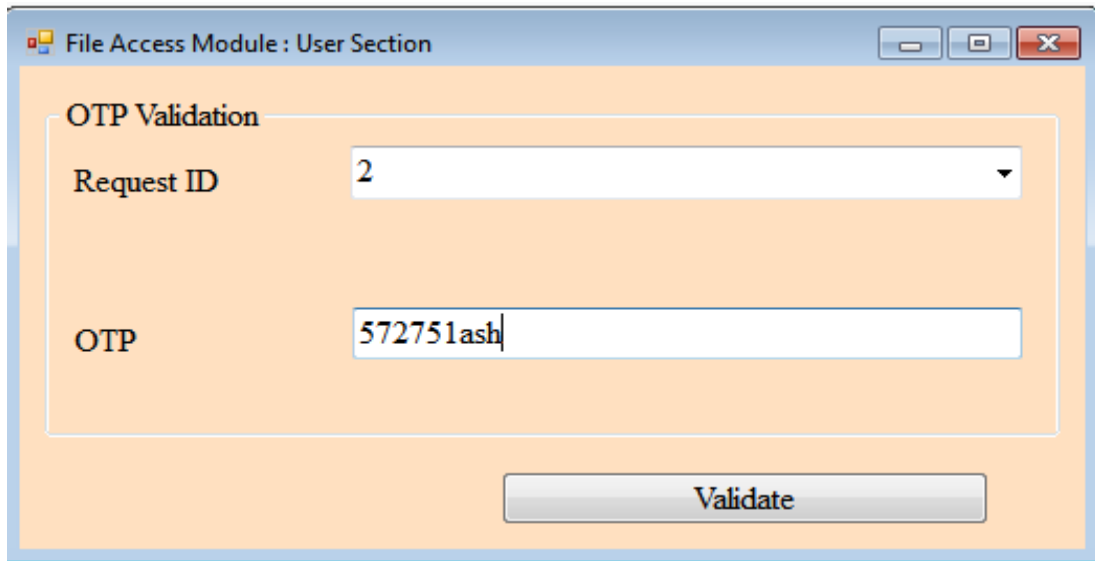


Figure 4: OTP Validation

After the validation of the request ID and OTP, the screen shows a file decryption form in which the decryption key is provided. The file chunks are then decrypted and joined.

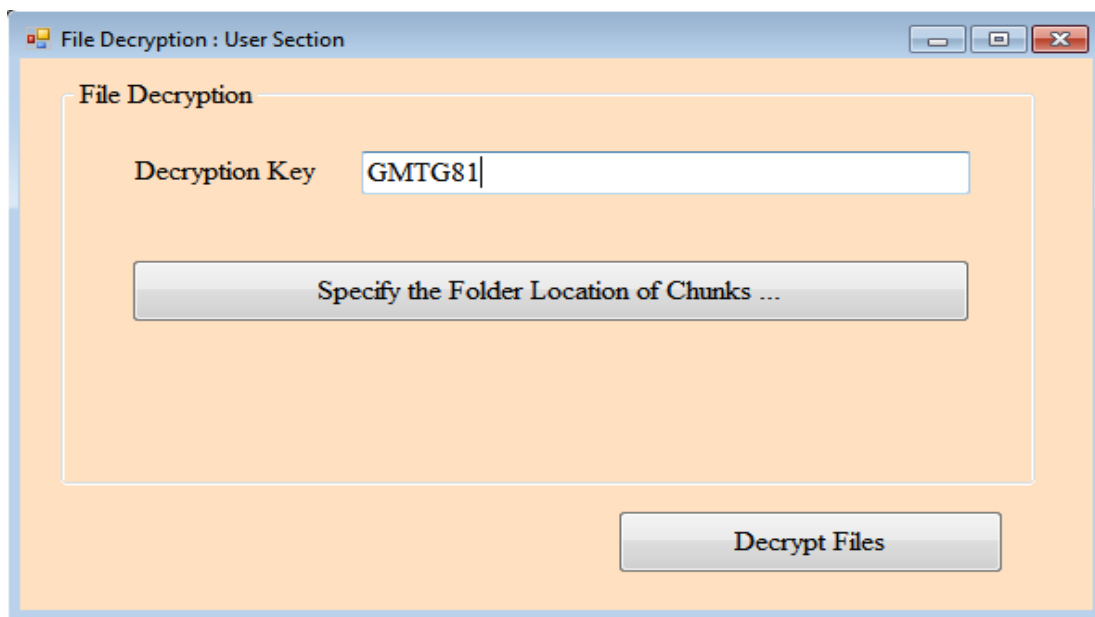


Figure 5: File Decryption using Encryption Key

V. Result Analysis

The concept of data access and storage which is proposed in the research we have done, has the following parameters for its evaluation.

1. TPA Based Security.
2. Data Transfer in Chunks

3. Encryption and Decryption of Chunks
4. Generation of OTP / Passcode for Access
5. Verification of Authenticity of Data.

TPA Based Security

It helps in two manners,

- a. It reduces the client load (that is the file owner) for granting and managing access to the data or files other user's request.
- b. TPA further acts as an interface for the validation of the users and maintains the checklist for the authorized users.

TPA further validates the user by issuing and managing request ID which is unique for all user requests and by the generation of the OTP based passcode for each access.

Data Transfer in Chunks

In order to smoothen the data transaction as when larger data is shared in a single file, chances of the data loss are more and will result in waste of time in retransferring of file again and again till it properly reaches the sender.

Suppose, consider the scenario where the system data transfer speed is 1 MB per sec and we have to transfer a file which is of 20 MB.

And the system is facing an issue where the connectivity is lost in every five seconds. And we have two scenarios,

Scenario 1: Single File is sent. In such a case that the file does not get sent, the connection gets lost in every 5 seconds and we will enter the loop where the file is required to be sent again and again.

Scenario 2: File is split into chunks of 2 MB and then these chunks are sent. In such a case, with 2 attempts of the transfer, all the chunks can be sent.

E.g. in each break, 10 mb of data is sent. So the 20 mb of file will be completely sent in 2 attempts.

Thus, the system is more reliable.

Encryption and Decryption of Chunks

The chunks of the files which are sent are encrypted and decrypted using the key based AES algorithm.

Generation of OTP / Passcode for Access

In the process, the passcode is generated for validating the user who has requested and as we have discussed in the earlier section, the encryption and decryption keys are also involved. Now, the matter arises regarding the strength of the keys and passcode which are used in the proposed work. So, in this section, we are making use of some tools for the validation of the password strength.

For the testing purpose we have used for the following keys which are generated in the process of the simulation of the proposed work.

Encryption Key:

S>%@S#

OTP/Password for File Requested:

677040ash>@

Tool 1: CrypTool

CrypTool is an open-source project which provides a free online learning software CrypTool demonstrating cryptographic and cryptanalytic thoughts.

Table 1 : Strength Analysis using Cryptool

	OTP Passcode	Encryption /Decryption Key
Score	100	61
Bit Strength	62	33
Entropy	3.096	2.252

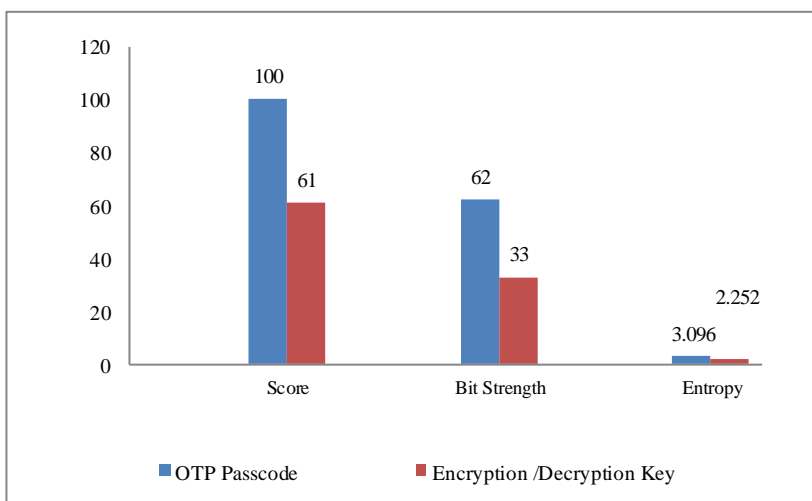


Figure 6: Examination of OTP and Key using Cryptool

Tool 2: zxcvbn test

zxcvbn is a password quality estimator propelled by password crackers. Through example coordinating and moderate estimation, it perceives and weighs 30k normal passwords, basic names and surnames as indicated by US statistics data, mainstream English words from Wikipedia and US TV and films, and other basic examples like dates, rehashes (aaa), groupings (abcd), keyboard designs (qwertyuiop), and l33t talk.

Table 2 : Strength Analysis using zxcvbn

	OTP Passcode	Encryption /Decryption Key

Entropy bits	35	19
--------------	----	----

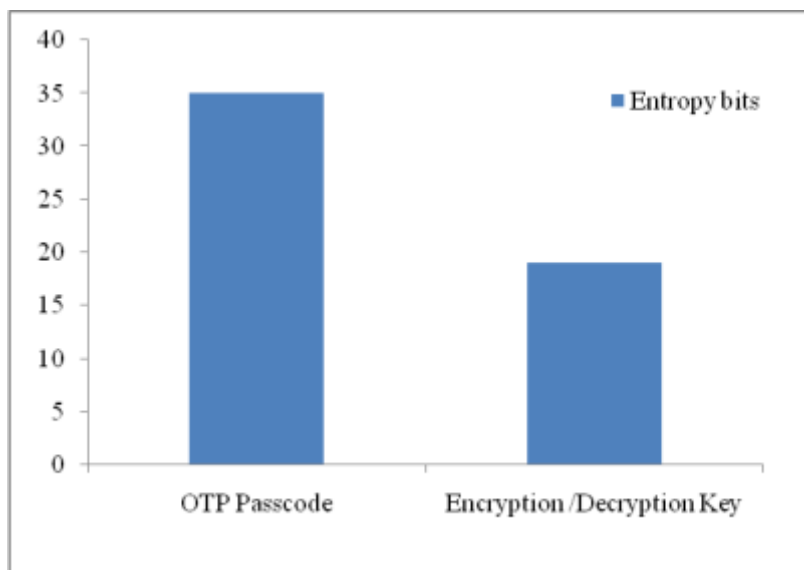


Figure 7: Examination of OTP and Key zxcvbn

VI. Conclusion

Data Access and Data Storage are becoming a vital issue for an organization. Necessary data is required to be accessed by the users and at the same time it is required that the data should be protected from unauthorized access. The proposed work is designed to solve such issues of an organization. The model relies on the TPA based security concept, which authenticates the request and manage and grant access to the files requested. The TPA will manage the access list for the data shared. With the TPA model it gives flexible storage system makes feasible and effective access of data in the form of chunks, thus maintaining the ease of the access with the data security by encrypting the chunks with dynamic keys. The integrity of the data shared is also managed by cross validation of the file hash at the receiver end and thus, in result provides a stable system for data sharing and data access. The keys used in the process are also tested for reliability using entropy checking tools, which are available online or offline and the result further ensure the stability of the system.

References

- [1] A.S. Kalyana Kumar, K. Abdul Razak, "A Secure Crypto-Based Data Outsourcing Model for Monitoring the Smart Environment in Cloud," *Int. J. Scient. Technol. Res.*, vol. 8, pp. 7-12, 2019.
- [2] R. Singh and S. Prakash, "Privacy preserving in TPA for secure cloud by using encryption technique," in *IEEE Int. Conf. Innovat. Inf., Embedded Comm. Sys. (ICIECS)*, March 2017, pp. 1-5.
- [3] J S. Hiremath and S. R. Kunte, "Ensuring Cloud Data Security using Public Auditing with Privacy Preserving," in *IEEE 3rd Int. Conf. Comm. Electron. Sys. (ICES)*, Oct 2018, pp. 1100-1104.

- [4] P. Kharmate and R. Suryawanshi, "Cloud Based Two Tier Security Scheme for Store, Share and Audit Our Data into Cloud," in *IEEE Int. Conf. Adv. Electr., Comm. Comp. Technol. (ICAECCT)*, Dec. 2016, pp. 116-121.
- [5] Bin Feng, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu, "An Efficient Protocol With Bidirectional Verification For Storage Security In Cloud Computing", in *IEEE Acc.*, vol. 4, pp. 7899-7911, 2016.
- [6] O. Heinisuo, V. Lenarduzzi and D. Taibi, "Asterism: Decentralized File Sharing Application for Mobile Devices," *IEEE Int. Conf. Mob. Cloud Comp. Serv. Eng. (MobileCloud)*, 2019, pp. 38-47.
- [7] M. A. Mohammed, Z. H. Salih, N. Țăpuș and R. A. K. Hasan, "Security and accountability for sharing the data stored in the cloud," *RoEduNet Conf. Net. Educ. Res.*, 2016, pp. 1-5.
- [8] S. Hiremath and S. Kunte, "A novel data auditing approach to achieve data privacy and data integrity in cloud computing," in *IEEE Int. Conf. Electrical, Electronics, Comm., Comp., Optimizat. Techniq. (ICEECCOT)*, Dec. 2017, pp. 306-310.
- [9] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," in *IEEE Trans Cloud Comp.*, vol. 5, issue. 3, pp. 523-536, 2017.
- [10] Z. Xia, X. Wang, X. Sun and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340-352, 1 Feb. 2016.
- [11] S. D. Thosar and P. Sonewar, "Data integrity verification privacy preserving approach of cloud using Third Party Auditor and multithreading," in *IEEE Int. Conf. Comput. Comm. Cont. Automat. (ICCUBEA)*, Aug. 2016, pp. 1-4.
- [12] I. El Ghoubach, R. B. Abbou and F. Mrabti, "A secure and efficient remote data auditing scheme for cloud storage," *J. King Saud Uni. Comp. Inf. Sci.*, 2019.
- [13] S. H. Abbdal, H. Jin, A. A. Yassin, Z. A. Abduljabbar, M. A. Hussain, Z. A. Hussien and D. Zou, "An Efficient Public Verifiability and Data Integrity Using Multiple TPAs in Cloud Data Storage," in *IEEE 2nd Int. Conf. Big Data Sec. Cloud (BigDataSecurity)*, *IEEE Int. Conf. High Perf. Smart Comput. (HPSC)*, and *IEEE Int. Conf. Intellig. Data Sec. (IDS)*, April 2016, pp. 412-417.
- [14] S. Hiremath and S. R. Kunte, "Ensuring Cloud Data Security using Public Auditing with Privacy Preserving," in *IEEE 3rd Int. Conf. Comm. Electron. Sys. (ICCES)*, Oct. 2018, pp. 1100-1104.
- [15] S. Patii and N. Rai, "An effectual information probity with two TPAS in cloud storage system," in *IEEE 3rd Int. Conf. Sci. Technol. Engineer. Manage. (ICONSTEM)*, March 2017, pp. 432-434.
- [16] A. K. Udagatti and N. R. Sunitha, "Fault tolerant public auditing system in cloud environment," in *IEEE 2nd Int. Conf. Appl. Theoret. Comput. Comm. Technol. (iCATccT)*, July 2016, pp. 359-362.
- [17] J. Raja and M. Ramakrishnan, "Public key based third party auditing system using random masking and bilinear total signature for privacy in public cloud environment," in *IEEE Int. Conf. Intellig. Comput. Cont. Sys. (ICICCS)*, June 2017, pp. 1200-1205.

- [18]S. Shaikh and D. Vora, "Secure cloud auditing over encrypted data," in *IEEE Int. Conf. Comm. Electron. Sys. (ICCES)*, Oct. 2016, pp. 1-5.