ISSN: 2278-4632
Vol-10 Issue-7 No. 2 July 2020

NOVEL APPROACH FOR TPA BASED DATA SHARING USING HASHING ALGORITHMS

[1]Ashish Bhardwaj, [2]Dr. Surendra Yadav

Research Scholar

[1]Career Point University

[2]Career Point University

[1]bhardwajashish739@gmail.com, [2] syadav66@gmail.com

[1]+91-8586927995, [2]+91-9982317251

ISSN: 2278-4632
Vol-10 Issue-7 No. 2 July 2020

ABSTRACT

In most of the organization the data is shared on the daily basis. The problems which are associated with the cloud environment is regarding smooth sharing of data and secure sharing. The sharing of the large piece of information is always of the bigger issue and the data lost will be their due to some network instructions. The second issue is the genuine validation of the user, so thatonly the authorized user will base to access data. This paper reviews the concept related to the secure file sharing using the concept highlighting with the base paper followed in the research work. In together to that, highlight the new approach of the file access using the chunks-based encryption and with the integrity check of the file send and received using the verification done by TPA. The bigger data is divided into parts so that no data loss will be there which occurs due to sending bigger data at a time. Now the number of divisions or parts will be regulated that is not so mart parts be created as it will be more time consuming to manage all parts and more be too less otherwise, we will get the same issues which we are facing with sending large files. With the involved of the third part, the more secure authentication for accessing the files will be provided using the parameters set by TPA. So, in this way the system provides the secure mode of sharing of files with the user in the trust environment governed by TPA.

Keywords: Secure File Share, SHA, TPA Monitoring

I. INTRODUCTION

Cloud storage is a prototype of Computer information storage in which the computerized information is put away in logical pools. The physical storage traverses' one or more servers, and the state of being is generally had and regulated by a facilitating association. Cloud storage is a cloud processing prototype in which information is put away on remote servers got to from the web, or "cloud." It is kept up, worked and administered by a distributed storage experts collaboration on a storage server that depends on virtualization procedures. [1]

Most business cloud storage administrations utilize immense quantities of hard drive storage frameworks mounted in servers that are connected by a work like system engineering. Specialist organizations have additionally added superior layers to their virtual storage contributions, commonly involving some sort of solid-state drives (SSDs). [2]

The security of cloud storage administrations keeps on being a worry among clients. Specialist co-ops have attempted to mollify those feelings of dread by upgrading their security abilities by consolidating data encryption, multi-factor authentication and improved physical security into their administrations. [3] Cloud-based web security is a redistributed answer for putting away data. Rather than sparing data onto nearby hard drives, clients store data on Internet-associated servers. Data Centres deal with these servers to keep the data protected and make sure about to get to.[4]

ISSN: 2278-4632
Vol-10 Issue-7 No. 2 July 2020

II. LITERATURE REVIEW

Bin Feng et. al 2016, [5] authors in this paper structure an assessment system which will be utilized for the cloud storage systems and which thus for the usage of a productive and dynamic privacy-preserving auditing protocol.[5] The authors stretched out the auditing protocol to help dynamic data processing, which saw as proficient in the random oracle model. The protocol additionally bolsters the bidirectional authentication and utilizes the better load distribution strategy, which helps in lessening the computational overhead of the customer. But some gaps which we have found in the paper, which forms the basis of our proposed approach are,

- provide data confidentiality in Amazon based cloud infrastructure storage services
- verify the authentication of assessing files and defending against attacks and byzantine failures
- develop a Novel Remote Integrity Verification Technique for verifying the cloud user.
- implement the Novel Data Block Integrity Verification model for providing the storage security
- develop a Novel Access Control Structure based policy Generation Technique for the restricted access of the stored data blocks by the cloud users.

M. A. Mohammed et. al 2016, [6] Cloud service provider module is to process information owner demand for storing data files and application and gives cloud end users log subtleties to information proprietor for review reason, to address this difficult structure dependent on data responsibility to follow along and preliminary of the true treatment of the clients' information in the cloud. the idea which is suggested by the composer is that the information can be completely traceable by the proprietor and data owners can catch up the service contracts to the premise of the different sorts of things like access, utilization control and the management.[6]

O. Heinisuo , et. Al 2019 , [7] In this paper the authors work with the likelihood to utilize the cell phones as the decentralized record sharing stage without utilizing any of the focal specialists. Authors accomplished this by the execution of the framework which they named Asterism, which is a Peer to peer file-sharing mobile application one which depends on the Inter-Planetary File System.

They approved the outcomes by deploying and afterward estimating up the application network utilization and power utilization by looking at that on the numerous various gadgets. The examination aftereffects of the created structure show that the cell phones can be utilized to execute the globally distributed file-sharing network. Be that as it may, the hole in the exploration work is

ISSN: 2278-4632
Vol-10 Issue-7 No. 2 July 2020

that the data sharing application produced a lot of network traffic in any event, when no records was the consequence of which the battery life of the gadgets was enormously degraded. [7].

III. PROPOSED APPROACH

This section corresponds to secure file sharing in the cloud based environment with the proper validation of the user.

In the phase of the validation of the user, we are also using the TPA which is the third part authenticator.

So the whole process of sharing includes,

- User Authentication
- User File Encryption
- Server Retrieval

User Authentication Algorithm

This section is the user validation for accessing the cloud services for the accessing or the retrieval of the data.

Step 1: First assigned the TPA [9] for the validation of the users.

Step 2: Access the list of the valid users for the service to validate the user requesting the service of the file access or file storage.

Step 3: In order to further double validate the identity of the user the random six digit OTP is generated with the 3 digits extract of the user id.

Thus, the general format of the OTP will look like,

R1R2R3R4R5R6X1X2X3

Where,

R1,R2,R3,R4,R5,R6 are the arbitrary numbers which can be any single digit value in the range of 0 to 9.

X1X2X3 are the first three digits extracts of the user id of the user requesting for the cloud service.

Step 4: The OTP generated will be send to the user requesting using the registered email id as well as to the registered mobile number.

ISSN: 2278-4632
Vol-10 Issue-7 No. 2 July 2020

Step 5: User then enter the OTP and send the OTP back for the validation by the TPA.

Step 6: If validated then Proceed for accessing the cloud services Else Go to Step 7.

Step 7: Stop.

User File Encryption and storage

To validate the virtue of the file, the concept we enhance is that we will generate the MD5 hash of the file send on the sender end and at the receiving end then the chunks are joined, the MD5 hash is again generated to cross check that both hash are same, if both the hash are same, then the file will be treated as authentic.

Step 1: Read the file, user name

Step 2: Select the column from the data loaded which determines the bases for the clustering.

Step 3: Create the Clusters of Special Characters, Lowe case alphabets, Upper case alphabets, Numbers and arrange on the basis of the size of the number of elements in the clusters.

Step 4: The Clusters are then segmented into the groups on the basis of the size of the elements in the groups.

Step 5: Every time the random cluster is selected from each group.

Step 6: Then the random password is generated and used for the key for encryption with the AES algorithm

Step 7: Store the details of the randomly selected cluster (assigned cluster ID with the sequence number) and key on the cloud server with the unique file id.

Step 7: Generate the Hash for the original file using the MD5 algorithm.

Step 8: Also store the file related hash with the unique file id on the cloud server.

Step 9: Stop.

File Retrieval

This section is used the user requesting the access for the file stored on the cloud server.

Step 1: Read the UserName (The process of the retrieval will be initiated only after the user validation or authentication is done).

Step 2: File ID requested, User has to provide the MD5 hash of the file requested.

Step 3: If server access the file using the File ID and access the MD5 hash of the file.

ISSN: 2278-4632
Vol-10 Issue-7 No. 2 July 2020

Step 4: If MD5 Hash match then Go to Step 5 Else Go to Step 14.

Step 5: Access the Cluster of the File ID.

Step 6: Prompt for the key on the basis of the Cluster ID.

Step 7: If Key validated then Go to Step 8 Else Go to Step 14

Step 8: Decrypt the cluster and store back the cluster.

Step 10: Rearrange all cluster and join the file.

Step 11: Calculate the MD5 hash of the resultant file. [Hash is generated here for integrity check]

Step 12: If same then Go to Step 13 Else Go to Step 14

Step 13: Grant access to the file and deliver the file.

Step 14: Stop.

IV. JUSTIFICATION OF PROPOSED APPROACH

According to the Synopsis and the base paper, the work which we proposed is in line of the TPA governed list for accessing to the stored data and bidirectional validation in the different way. The concept which we have proposed works in the three segments ,

1. User Authentication
2. User File Encryption
3. Server Retrieval

The authorized list of users is maintained in the system, as to access the system, first of all users required to be registered. Now, the proposed work, works in the line of the TPA audit, for which proposed system will maintain the separate section for the TPA login [10], to filter out the user list who can access the file or the data which is being shared in the system.

For the following gaps,

- To provide data confidentiality in Amazon based cloud infrastructure storage services
- To verify the authentication of assessing files and defending against attacks and byzantine failures
- To develop a Novel Remote Integrity Verification Technique for verifying the cloud user.

The proposed work works in the following manner,

ISSN: 2278-4632
Vol-10 Issue-7 No. 2 July 2020

- Division of larger file / data into chunks or the clusters for the smooth transfer.
- Now for the security of the data not being guessed up by the hackers, the splited file is randomly selected for the sending phase , in the random sequence of the clusters.,
- For the security of the data each cluster is encrypted using the AES algorithm in which key is the randomly generated password.
- Now working for the bidirectional validation, in this we have generated the SHA code for the file which is being shared. SHA code for the file is unique. So , in the receiver module when the file is decrypted after all the validation checks , the SHA code is again generated for the decrypted file and if the send file SHA and the decrypted file SHA are same then only the file is validated for download or further use purpose.

And for the gaps,

- To implement the Novel Data Block Integrity Verification model for providing the storage security
- To develop a Novel Access Control Structure based policy Generation Technique for the restricted availability of the stored data blocks by the cloud users.

The proposed work, works in the following manner following the user authentication algorithms in which the TPA is also involved and for TPA the separate section is created and the TPA will manage the list of the user who can access that data if the user who is not in the list will tries to access or decrypt the file , access is denied.

The task of the assignment of the users for the particular file access is discussed in the algorithm,

And the unique identification key is devised for the verification of the user for the file access for the purpose of same the following concept is used,

In order to further double validate the identity of the user the random six digit OTP is generated with the 3 digits extract of the user id.

Thus, the general format of the OTP will look like,

R1R2R3R4R5R6X1X2X3

Where,

ISSN: 2278-4632
Vol-10 Issue-7 No. 2 July 2020

R1,R2,R3,R4,R5,R6 are the arbitrary numbers which can be any single digit value in the range of 0 to 9.

X1X2X3 are the first three digits extracts of the user id of the user requesting for the cloud service.

And the user of this list is reflected in the file retrieval also as the user when request for the file, the user first request for the file for which a unique request id is generated and in the user validation form, in which the request id is first required to be selected (generated in the file request phase by the user requesting for the access) and the user data is checked for the details of the user and then also checked for whether the user has been granted the access for the file requested. If all the details are ok , then the "Eligible for access" section will show Yes and the OTP is then send.

V. CONCLUSION

The proposed approach provided the significant approach for overcoming all the gaps which are highlighted in the paper, the next step which we will proceed will be the implementation of the model proposed and for the simulation purpose, we are planning to done the implementation in Visual Studio and for the database required for that will be implemented in SQL Server.

REFERENCES

[1] Sookhak, M. (2015). Dynamic remote data auditing for securing big data storage in cloud computing (Doctoral dissertation, University of Malaya).

[2] Yu, J., Ren, K., Wang, C., & Varadharajan, V. (2015). Enabling cloud storage auditing with key-exposure resistance. *IEEE Transactions on Information forensics and security*, 10(6), 1167-1179.

[3] Wang, C., Wang, Q., Ren, K., & Lou, W. (2010, March). Privacy-preserving public auditing for data storage security in cloud computing. In *2010 proceedings IEEE infocom* (pp. 1-9).

[4] Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2015). Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds. *IEEE Transactions on Cloud Computing*, 5(3), 523-536.

[5] Feng, B., Ma, X., Guo, C., Shi, H., Fu, Z., & Qiu, T. (2016). An efficient protocol with bidirectional verification for storage security in cloud computing. *IEEE Access*, 4, 7899-7911.

ISSN: 2278-4632
Vol-10 Issue-7 No. 2 July 2020

[6] Mohammed, M. A., Salih, Z. H., Ţăpuş, N., & Hasan, R. A. K. (2016, September). Security and accountability for sharing the data stored in the cloud. In *2016 15th RoEduNet Conference: Networking in Education and Research* (pp. 1-5).

[7] Heinisuo, O. P., Lenarduzzi, V., & Taibi, D. (2019, April). Asterism: Decentralized File Sharing Application for Mobile Devices. In *2019 7th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* (pp. 38-47).

[8] Xia, Z., Wang, X., Sun, X., & Wang, Q. (2016). A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. *IEEE transactions on parallel and distributed systems*, *27*(2), 340-352.

[9] Paladi, N., Gehrmann, C., & Michalas, A. (2016). Providing user security guarantees in public infrastructure clouds. *IEEE Transactions on Cloud Computing*, *5*(3), 405-419.

[10] Schiffman, J., Moyer, T., Vijayakumar, H., Jaeger, T., & McDaniel, P. (2010, October). Seeding clouds with trust anchors. In *Proceedings of the 2010 ACM workshop on Cloud computing security workshop* (pp. 43-46).

[11] Paladi, N., Michalas, A., & Gehrmann, C. (2014, June). Domain based storage protection with secure access control for the cloud. In *Proceedings of the 2nd international workshop on Security in cloud computing* (pp. 35-42).

[12] Jordon, M. (2012). Cleaning up dirty disks in the cloud. *Network Security*, *2012*(10), 12-15.

[13] Michalas, A., Paladi, N., & Gehrmann, C. (2014, October). Security aspects of e-health systems migration to the cloud. In *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)* (pp. 212-218).

