Light Weight Cloud Storage Auditing With De-Duplication Supporting Strong Privacy Protection

Gopinath A R [1], Shivam Kumar Lal [2], Suruchi Neupane [3], Sumit Kumar [4]

[1] *Associate Professor, Department of Computer Science and Engineering, NagarjunaCollegeof Engineering and Technology, Bangalore, India*

[2, 3, 4] *B.E. Students, Department of Information Science and Engineering, NagarjunaCollegeof Engineering and Technology, Bangalore, India*

Abstract: ***We present a new approach of the 2FA to provide security to the data user using the concept of light weight. In our paper, 2FA technique is implemented with the exigency of the user where he/she needs both the secret key as well as the light weight security device. It enhances the reliability of the system as the user needs to enter both the keys correctly, especially in those cases where many users share the same system for different web-based cloud services. In addition, it also used the concept of de- deduplication where it removes extra copies of the same kind of files, leaving only a single copy to be stored.***

Keywords: 2FA, Cloud Computing, Light Weight Device, Encryption & Decryption, de-duplication.

I. INTRODUCTION

The main goal of our project is to accomplish the security by delivering two factor authentication using the concept of light weight where we are conceptualizing deduplication to delete the files having multiple copies of same data, leaving only one single copy of the file to be stored**.** Cloud computing is referred as the server that have access over the internet, present at remote location where we will restore the data and the stored data are processed and managed in the server itself in cloud those stored data can be accessed anytime and anywhere by the user. Cloud computing is all about sharing of different resources to achieve comprehensibility. Cloud computing gives permission to user to access the application without performing any hard work through the Internet. It is based on the technique of pay-per- use model which means the clients only have to pay for what they have used which eliminates the extra cost. In addition, it also provides the on demand services which means that the clients can access the data from anywhere, any place and anytime. It might be available for any enterprise or, limited to a single organization. In today's digital world almost millions of data are uploaded in the cloud every day. So it is very important to develop a cloud storage auditing so that any user may verify the probity of data, without downloading it from the cloud. And also, lots of copies of data are stored for the same data on the cloud. Hence, it's very crucial to extract duplicate data from the cloud. So it does not affect the storage and increase the efficiency of the cloud.

II. LITERATURE SURVEY

The aim of literature survey is to layout additional information on the issues to be regarded in this thesis and to focus more on the importance of current study. This chapter depicts the study of the related technologies and summary of the related work done in the past.

- Attribute Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud

[1] Attribute based encryption is largely accepted in cloud computing. This is a platform where outside supplier will provide their data which is in the encrypted form to cloudservices. They can also interchange them with any users having particular attributes. As we are using deduplication for deleting the extra copies of same file to minimize the space and also network

Bandwidth, this deduplication is not securely supported by standard ABE system. In order to manage our storage space we are providing an attribute based storage with secure deduplication in a hybrid cloud setting where detecting the duplicate file is to be performed by private cloud and the space is taken care by the public cloud.

We will have two advantages if we compare our system with previous data deduplication systems. First advantage is, instead of sharing those decryption keys here directly we can share any data confidentially by providing access rules with users. The second advantage is, we achieve the standard idea of explication security for data secretiveness while existing systems only achieve it by defining a delicate security ideas.

- Lightweight Privacy-Preserving Identity-Based Verifiable IOT-Based Health Storage System [2] The IoT is also very useful in health sector. We can use IoT devicest o provide smart health systems in an intelligent way. We can use devices that are based on IoT to enable the examination of remote health system and also can be used for emergency purpose during treatment of any patient. These devices are used to monitor the improvement of the patients having any sort of health issues. This devices provides a better health facilities using a network that connects the doctor and patients throughout the treatment. With the help of IoT. We can also organize the different medical reports or health related data in a systematic order that can be easily accessed. IOT devices uses different sensors, microcontroller, WIFI- modules and cloud based web applications to achieve the secure health system in an intelligent way which results in better health system.

III. PROBLEM STATEMENT

In a common cloud surrounding where people generally work in spinning shifts, the consolidate system may be used by abounding users & decumbent to be at risk. It will be accessible for the operator to introduce any spyware & get to notice the login id & passwords. In today's world, even if a system is locked by any secured password, it is possible for the hackers to get into our system or guess the password and get to know our confidential data.

IV. PROPOSED SYETEM

The main objective of our work is to illustrate how we can covenant security by providing two factor authentication using the concept of light weight and the deduplication concept to demolish the extra copies of the same file, ending up displaying only the unique copy of the file. Here, we survey how to obey the brute force dictionary attacks entirely and apprehend deduplication with secure privacy in cloud storage auditing. We propose the 2FA (two- factor authentication) to enhance the security control of the system in different cloud- computing services. We are also using the concept of light- weight security key. Our proposed system includes the following two cases.

Case 1: Authentication key:-

The secret key is sent to the mail id of the user, which he provides when the data trustee creates the data user. This key is called the pseudonym key. This is used for the authentication purpose i.e. whether he belong to the organization or not.

Case 2: Access-Control key

The user again will be carrying the security key in a light weight service. This is also called as the private key. This key is for the access control like to which specific department and designation the file has to be uploaded.

Thus, the user needs to enter both the keys correctly. Access is given for download only where both the keys are correct or else, access is denied. Also, de-duplication concept is also used here, in which extra copies of the same data is eliminated, leaving only a single copy to be stored.

V. SYSTEM DESIGN

The System Design of our work is dividedinto 3 modules i.e.

- Authority
- Trustee
- User

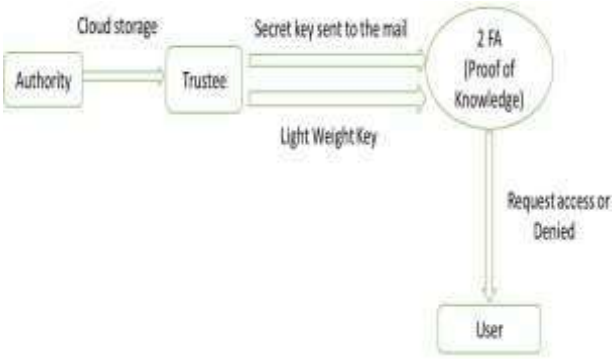


Fig 1: System Block Diagram

- **Authority**

Authority is a magnificent admin who constitutes the Data Trustee and preserves the cloud server's compositions. He can Add, Edit or Delete any figure of Trustee. He can also approach to cloud storage, data trustee, key formation, department, designation and also adjustment password.

- **Trustee**

Trustee is one who will stock the data in cloud which can be accessed by the authorized Customers. Trustees are like Liberian who will transfer all the files in the arrangement. Whenever the file is transfer it will be encrypted by the arrangement using Trustee Encryption Key. He has the approach to fill the user particulars, generate the aspect based key (ABK), details of the user, cipher the ABK with DNA Algorithm, mail the key to the customer, change password.

User

Data users are nothing but the data access customers, like Trustee is a college Liberian then data consumers are like students, lectures and admin staff in a college. Data Consumer receives the access key (Attributed based Decryption Key) from the Trustee through email and light weight security device.

Algorithms used:

- **AES Algorithm** (Advanced Encryption Algorithm): AES, also acknowledged as Rijndeal whichis used for encryption and decryption of the computerized data. It works on dominant of substitution- permutation organization and is applicable for both software as together as hardware. It's block sizes are 128, 192 0r 256 bits . In our project we have used this AES algorithm for the generation of key as well as for the encrypting the file while deploying in the cloud.

- **DNA Algorithm:** DNA stands for Deoxyribonucleic Acid. It is a hereditary algorithm which is recycled for the verification aspiration. DNA Encryption is a development of hiding or changing genetic information by computational methods for better genetic privacy in DNA sequencing processes. In our project, we used this algorithm for the genetics hereditary like making the relation between the authority and the trustee.

- **MD5 Algorithm** (Message-Digest Algorithm)**:** This algorithm uses the hashing function to produce 128-bit hash value. It is a Cryptographic hashing algorithm which is used to verify the integrity of files. In our project we used this algorithm to make our project more secure and integrity, along with that we used this algorithm for the redundancy of duplicate file

  i.e. deduplication.

VII. RESULTS



Fig 2: Admin login Page



Fig 3: Trustee login Page



Fig 4 : User login page

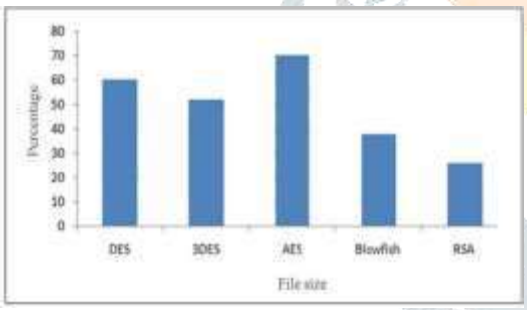


Fig 4: Avalanche Effect Bars

Fig 5 demonstrates the comparison of AES Algorithm with different algorithm techniques for encrypting data. This figure shows the relationship between the file size of the data vs the accurate percentage with which the data gets encrypted. CONCLUSION

We proposed the idea of the 2FA (which includes both the secret and the light weight key) for different web-based cloud services. It enhances the security of the system especially for those system where the system is shared in different web-based cloud services. And also, duplicate files are deleted from the cloud, leaving only a single or unique copy of file to be stored,which does not affect the storage.

REFERENCES

[1] Attribute Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud.

[2] Lightweight Privacy-Preserving Identity-Based Verifiable IOT-Based Health Storage System.

[3] One secure data integrity verification scheme for cloud storage.

[4] Side Channels in Cloud Services: Deduplication in Cloud Storage.

[5] Cloud storage auditing with deduplication supporting different security levels according to data popularity

[6]
https://ieeexplore.ieee.org/document/9020052
[7]
https://www.researchgate.net/publication/339634904_Lightweight_Cloud_Storage_Auditing_With_Deduplication_Supporting_Strong_Privacy_Protection.
[8]
https://www.semanticscholar.org/paper/Lightweight-Cloud-Storage-Auditing-With-Supporting-Shen-Su/17ef213b1b28e6dcfb0529b0c90b5b86065c210f
[9]
https://www.hindawi.com/journals/wcmc/2021/8886763/
[10]
https://abtechnologies.in/project/lightweight-cloud-storage-auditing-with-deduplication-supporting-strong-privacy-protection