https://doi.org/10.46335/IJIES.2022.7.9. 18 **e-ISSN: 2456-3463**
Vol. 7, No. 9, 2022, PP. 92- 96

International Journal of Innovations in Engineering and Science, www.ijies.net

Enhancing the Cloud Security via Cryptography

Jagruti Mahajan[1], Harshada Rathod[2], Parul Mankar[3] Monika Korde[4], Vaishnavi Rathod[5], Professor Kalyani Pendke[6]

Rajiv Gandhi College of Engineering and Research, Nagpur, India,441110 Department of Computer Science& Engineering,

jagrutimaha2000@gmail.com

***Received on**: 11 June ,2022* ***Revised on**: 07 August ,2022* ***Published on**: 09 August,2022*

Abstract-*Cloud computing facilitates different cloud services in which the most popular one is cloud storage. Data holders store their data in a cloud server, here the use of cloud servers is growing daily. A huge amount of data daily get uploaded to the cloud server. One important thing that needs to be focused which is security. Our proposed work is nothing but to let the data holders feel safe about data on the cloud by providing security. For maintaining the privacy and security of data, in our project, the data holders store their data by using encryption and decryption. Another big issue related to the cloud is that data duplication. Because of this issue server storage, cost, environment, and other factors are increasing. Here in our proposed work, we will provide the solution for this issue also. Here, we have proposed a data Deduplication concept with the SHA1 algorithm. By implanting both these concepts we are providing a solution to two big problems of the cloud.*

Keywords: *Cloud Computing, Security, Cryptography, AES algorithm.*

I- INTRODUCTION

Cloud storage has emerged as a promising solution for providing ubiquitous, convenient, and on-demand access to large amounts of data shared over the Internet [1]. However, whereas enjoying the convenience of sharing information via cloud storage, users are progressively involved regarding un intended information leaks within the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets (example: the recent high-profile incident of celebrity photos being leaked on iCloud) [3].

To address users' concerns over potential data leaks in cloud storage, a common approach is for the data owner to encrypt all the data before uploading them to the cloud, such that later the encrypted data may be retrieved and decrypted by those who have the decryption keys. Such cloud storage is often called cryptographic cloud storage. Although combining an encryption scheme with cryptographic cloud storage can achieve the basic security requirements of cloud storage, implementing such a system for large scale applications involving millions of users and billions of files may still be hindered by practical issues involving the efficient management of encryption keys, which, to the best of our knowledge, are largely ignored [3].

First of all, the need for selectively sharing encrypted data with different users (e.g., sharing a business document with certain colleagues on a cloud drive) usually demands different encryption keys to be used for different files. However, this implies the number of keys that need to be distributed to users, both for them to search over the encrypted files and to decrypt the files, will be proportional to the number of such files. Such a large number of keys must not only be distributed to users via secure channels but also be securely stored and managed by the users on their devices. In addition, a large number of trapdoors must be generated by users and submitted to the cloud to perform a keyword search over many files. The implied need for secure communication, storage, and computational complexity

https://doi.org/10.46335/IJIES.2022.7.9. 18 **e-ISSN: 2456-3463**
Vol. 7, No. 9, 2022, PP. 92- 96

International Journal of Innovations in Engineering and Science, www.ijies.net

may Multi-Key Searchable Encryption In the case of a multi-user application, considering that the number of trapdoors is proportional to the number of documents to search over to the server a keyword trapdoor under each key with which a matching document might be encrypted [3].

Problem Definition: The client's concern about data security, data integrity, and sharing data with a specific band of men and women must be addressed. You can find multiple means of achieving this, for example encrypting data on the client machine and then storing the information on to cloud storage server, computing the hash of the information on the client machine, and storing a hash of data in the client machine, a client trying out the responsibility of sharing the trick key about encryption with a specific band of people [5].

Therefore it becomes more tedious for the client to keep this information and share such information, moreover in the event the device which stores such information is lost or stolen it poses a threat to the total data [4]. Another way could be the same storage cloud provider providing the service for secured sharing, hashing, and encryption/decryption. Therefore mentioned approaches burden the client which to makes it additionally accountable for securing its data before storing it in the cloud storag**e.**

II- PROBLEM STATEMENT

The current existing system is cloud servers. Here data owner will upload data to the cloud in human-readable file formats. That data as per requirement users can search and download. The best real-time example where we can take that is Google drive. On google drive, the user will select files from the system and upload them, and will make a logout. Now suppose his Gmail password gets hacked so that the hacker can make login to his Gmail and there on the drive he can get all files uploaded by the user. This is all about the existing system where the data of the user is unsafe.

III- SOME DEFINITIONS AND CONCEPTS

A. Cloud Computing:

Cloud computing is a general term for anything that involves delivering hosted services over the Internet [6].

Wikipedia defines cloud computing as:

"The delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices" [7].

B. Security

The major 4 security concerns are:

1) Secure data transfer
2) Secure software interfaces
3) Secure stored data
4) Secure User access control

B.1 Secure data transfer

All of the traffic traveling between your network and whatever service you're accessing in the cloud must traverse the Internet. Make sure your data is always traveling on a secure channel; also, your data should always be encrypted and authenticated using industry-standard protocols, that have been developed specifically for protecting Internet traffic.[8]

B.2 Secure software interfaces

The Cloud Securing Alliance (CSA) recommends that you just remember the package interfaces or APIs, that the area unit is accustomed move with cloud services [8].

B.3 Secure stored data

Your data should be securely encrypted when it's on the provider's servers and while it's in use by the cloud service [8].

B.4 User access control

Data stored on a cloud provider's server can potentially be accessed by an employee of that company, and you have none of the usual personnel controls over those people [8].

C. Cryptography: The art and science of concealing the messages to introduce secrecy in information security are recognized as cryptography. The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing [9].

Modern Cryptography: Modern cryptography is the cornerstone of computer and communications security. Its foundation is based on various concepts of mathematics such as number theory, computational complexity theory, and probability theory. Cryptography deals with the actual securing of digital data [9].

https://doi.org/10.46335/IJIES.2022.7.9. 18 **e-ISSN: 2456-3463**
Vol. 7, No. 9, 2022, PP. 92- 96

International Journal of Innovations in Engineering and Science, www.ijies.net

Cryptosystems: A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

IV. PROPOSED SYSTEM

In the proposed system data owner will upload data to the cloud server in an encrypted format. To perform encryption and we have used the AES algorithm here. There are two modules, user and admin, admin will be responsible for uploading files to the cloud and another will be the user who will be responsible for downloading files from the cloud. At first, the admin will make a login into his account and will select files, encrypt those files, and will upload that on CLOUD.

Now that files are there on CLOUD but in an encrypted format, suppose one of the users makes login to the account and searches existing files on CLOUD. There he got some files and that user is interested to download that files. To download the same he will need a decrypted key that he will send a request to the data owner or admin. Now admin will check the request and will send the decrypted key to that particular user on his Email. As the user will get that decrypted key on email now he will enter that and will decrypt and download files.

In this way, we will provide security to users via Encryption and decryption. When the admin will upload files on

V- PROPOSED METHODOLOGY

At the very first admin needs to upload data to the server at that time he will be asked to submit a secret key that secret key he can get from a project only and then he can submit it there. Once the admin has submitted the key the selected file will get decrypted and then it will ask whether to upload on the server or not to upload the encrypted file he needs to press the button. Here now user's work start. The first user will check the uploaded files on a cloud server. He will select a CLOUD that will be given to the SHA1 algorithm it will create one unique hash key for that and that hash key will be stored in a database. Now next time another user will try. particular document from that and will send a request to get the decrypt key for the document. That request will be received by the data owner or admin and now the owner will send a particular key for a particular document via mail.

Now user needs to check his email where he will get his secret key to download the document. The next user will submit the secret key and he will get the decrypted document. Now again he will be asked for download to download the same file admin needs to click the download button. The next most important part is when the user will upload a document on the server it will prevent uploading duplicate copies.

If the upload same file then that file's hash key will be checked with the saved hash key and if it gets matched then the duplicate copy will not be stored instead only one copy will remain there. This way we will avoid duplication of files on the cloud.

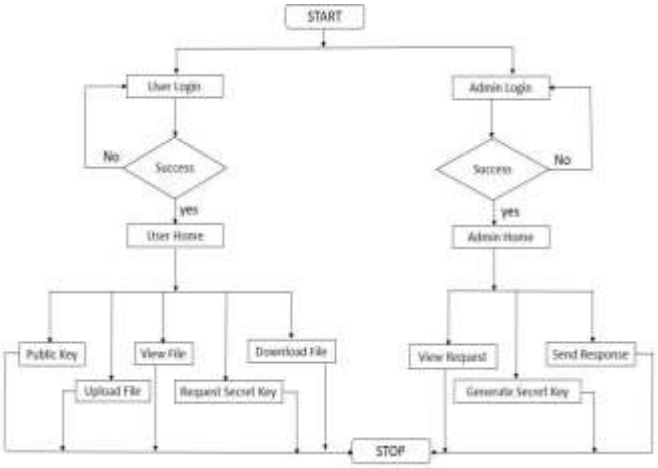

Fig.1: Architecture Diagram of the proposed system

VI- RESULTS

Fig 2: Encrypted Pag

Fig 2: In fig 2 user gets his file encrypted using the public key. He will not able to view the file until he downloads it.

https://doi.org/10.46335/IJIES.2022.7.9. 18 **e-ISSN: 2456-3463**
Vol. 7, No. 9, 2022, PP. 92- 96

International Journal of Innovations in Engineering and Science, www.ijies.net

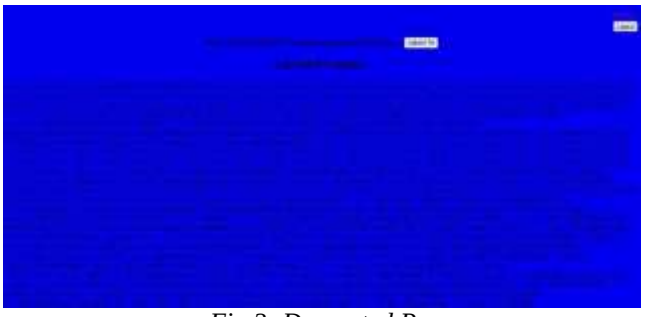

Fig 3: Decrypted Page

Fig3: In the above figure user will download the uploaded file on the server with the help of a secret key which he will get from the admin by sending him a request for a secret key. Users will be able to view the file because it is downloaded in Decrypted.

VII - CONCLUSION & FUTURE SCOPE

1. Conclusion

Our proposed system will be very much effective to support pollution by decreasing the size of CLOUD servers. We are solving the issue of wastage of storage also because of this our proposed System. By implementing both concepts of AES and SHA1 we will be improving the drawbacks of the existing system. Here now users can easily upload files without getting afraid of data leakage. Taking into consideration of the real problem of a privacy-preserving data sharing system based on public cloud storage which needs a data owner to allocate a key to users to permit them to access the documents, this proposed concept constructed a secure cloud scheme.

2. Future Scope

This implies that there are still tremendous opportunities for researchers to make fundamental contributions in this field, and make a significant impact on the advancements in cloud computing. Many key solutions in this domain are still in their infancy, such as automatic resource provisioning, cross- cloud services, novel fog- and IoT-based cloud services, and cloud modeling.

There is a scope to propose the guidelines to overcome future challenges like physical security, espionage, data ownership, hypervisor viruses, and malicious insiders in Cloud security. Despite the significant development in cloud computing, the current technologies are not yet mature enough to realize fully the potential of true utility computing. To concentrate on more specific areas like regulatory and compliance issues, jurisdiction laws, and many more. Cloud computing is about to realize the dream of computing as a utility.

REFERENCES

[1] *Pallavi Vijay Nichal , Prof. P. L. Ramteke, "A Survey On Cryptographic CLOUD Storage with Key Aggregate Searchable Encryption",(IJESRT)International Journal Of Engineering Sciences and Research Technology, March 2016, Amravati, India*

[2] *Kasthuri and R.Dharmarajan, "Agriculture Design Method Using Computing Architecture on Internet of Things", Journal on Science Engineering and Technology Vo1ume 5, No. 04, October 2018, Elambalur , Perambalur*

[3] *A.Pramod Kumar, S.M. Roy Choudri, "Key-Cumulative Reachable Encryption (CRSE) for Group Data Sharing via Cloud Storage", International Journal of Advances in Arts, Sciences and Engineering, Volume 4 Issue 9 Sep 2016 2320-6144 (Online), Guntur-522438, A. P., India*

[4] *Sajay Kr, Dr. Suvanam Sasidhar Babu, "Enhancing the security of cloud data using hybrid encryption algorithm", Springer, Journal of Ambient Intelligence and Humanized Computing,July 2019*

[5] *Nicholas Katende, Cheruiyot Wilson, Ann Muthoni Kibe, "Enhancing Confidentiality and Integrity in Cloud Computing using RSA Encryption Standard and MD5 Hashing Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 181 – No. 14, September 2018*

[6] *https://www.techtarget.Com/searchcloudcomputing/ definition/ clo ud-computing#:~:text=Cloud%20computing%20is%20a %20general, as%20a%20service%20(SaaS).*

[7] *https://www.computerworld.com/article/247278 2/ defining- cloud-computing--part-one-- laymen-s-terms.html*

[8] *https://www.vskills.in/certification/tutorial/threats-and-security- risks/*

[9] *https://www.tutorialspoint.com/cryptography/or origin_of_ cryptography.htm/, https://www.tutorialspoint.com/cryptography/modern _cryptograp hy.htm*

[10] *SRath, A., Spasic, B., Boucart, N., & Thiran, P.*

"Security pattern for cloud SaaS: From system and data security to privacy case study in AWS and azure." Computers, 8(2), 1–9. https://doi.org/10.3390/computers8020034

[11] *Thirukkumaran. R, Muthu Kannan. P, "Survey: Security and Trust Management in Internet of Things", Proceedings of the IEEE©2018, Chennai, TamilNadu*

[12] *Raed M. Salih Leszek T. Lilien, "Protecting Users' Privacy in Healthcare Cloud Computing with APB-TTP", Proceedings of the IEEE ©2015, Kalamazoo, MI 49008, USA*

[13] *Meryeme ALOUANE, Hanan EL BAKKALI, "Security, Privacy and Trust in Cloud Computing: A Comparative Study", Proceedings of the IEEE ©2015, Morocco*

[14] *Manish H. Gourkhede, Deepti P. Theng, "Analysing Security and Privacy Management For Cloud Computing Environment", Proceedings of the IEEE ©2014, Nagpur, Maharashtra,India*

[15] *Haifeng Li, Liangliang Liu, Caihui Lan, Caifen Wang, And He Guo, "Lattice-Based Privacy-Preserving and Forward-Secure Cloud Storage Public Auditing Scheme", Proceedings of the IEEE ©2020, China*

[16] *Thilakanathan, D., Chen, S., Nepal, S., & Calvo, R. A. "Security, Privacy and Trust in Cloud Systems" Secure Data Sharing in the Cloud In S. Nepal & M. Pathan (Eds.), 2014*

[17] *L. Lamport, "Password authentication with insecure communication", Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1981.*

[18] *Khan, A. N., Kiah, M. L. M., Madani, S. A., Ali, M., Khan, A. R., & Shamshirband, S. "Incremental proxy re-encryption scheme for mobile cloud computing environment", © Springer Science+Business Media New York 2013, J Supercomput DOI 10.1007/s11227-013-1055-z, Published Online 30 November 2013*

[19] *Weinhardt, A. Anandasivam, B. Blau, N. Borissov, T. Meinl, W.Michalk, and J. Stober, "Cloud computing ? a classification, business models, and research di- 29 rections", Business & Information Systems Engineering (BISE), vol. 1, no. 5, pp. 391-399, 2009.*