e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

SECURE FILE STORAGE ON CLOUD USING ELLIPTIC CURVE CRYPTOGRAPHY (ECC) ALGORITHM

Vedita Santosh Mhatre*1, Sadaf Naaz Shakeel Patel*2

*1,2Department of IT (Information Technology), S.I.W.S College, Mumbai, India

DOI : https://www.doi.org/10.56726/IRJMETS33137

ABSTRACT

Cloud is used in various fields like industry, military, college, etc. for various services and storage of huge amount of data. Data stored in this cloud can be accessed or retrieved on the users request without direct access to the server computer. But the major concern regarding storage of data online that is on the cloud is the Security. This Security concern can be solved using various ways, the most commonly used techniques are cryptography and steganography. But sometimes a single technique or algorithm alone cannot provide high-level security. Cloud storage services may be accessed through a web service API through a Web-based user interface. The cloud storage architectures build a single virtual cloud storage system or cloud of clouds system.

Keywords – Cloud Computing and Storage, Modified RSA Algorithm, ECC Algorithm, Blowfish Algorithm.

I. INTRODUCTION

Cloud storage providers operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualizes the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams [1]. Cloud storage is simply a term that refers to online space that you can use to store your data. As well as keeping a backup of your files on physical storage devices such as: external hard drives, sub flash drives, etc. Cloud computing is used in many areas like industry, military colleges etc to storing huge amount of data. We can retrieve data from cloud on request of user. To store data on cloud we have to face many issues. To provide the solution to these issues there are n number of ways. Cryptography and steganography techniques are more popular now a day's for data security. Use of a single algorithm is not effective for high level security to data in cloud computing .[2]. Example of cloud computing: Amazon Cloud Drive, G Space, Minus, Web e-mail providers like Gmail, Hotmail and Yahoo! Mail store e-mail messages on their own servers, A DriveYouTube, Social networking sites like Face book and MySpaceSites like Flicker and Picasa host millions of digital photograph. As with any storage system, there are certain security properties that are desirable in a cloud storage system: confidentiality, integrity, write-serializability and read freshness. These properties ensure that user's data is always secure and cannot be modified by unauthorized users and the data is always at the latest versions when being retrieved by the user. [3] Storing important data with cloud storage providers comes with serious security risks. The cloud can leak confidential data, modify the data, or return inconsistent data to different users. This may happen due to bugs, crashes, operator errors, or misconfigurations. Furthermore, malicious security breaches can be much harder to detect or more damaging than accidental ones: external adversaries may penetrate the cloud storage provider, or employees of the service provider may commit an insider attack. [4] These concerns have prevented security conscious enterprises and consumers from using the cloud despite its benefits [5].

Cloud storage also help in immediate data exchange, thus giving access to multiple people. This makes this service a perfect tool for both distant and in-house work. Thus, online cloud storage and is beneficial for all types of businesses. Cloud storage is a more cost-efficient platform that does not require a huge investment and it can be actively used for connecting and collaborating with clients and employees. Hence more and more users are turning to cloud storage, making it a very popular alternative to traditional storage option.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

II. SYSTEM BENEFITS OF SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

[1] Data EncryptionData you store on a cloud can be encrypted either before or after you send it, providing added protection. There is a range of cloud storage security options, including Single Sign-On (SSO), Multi-Factor Authentication (MFA) and more.

[2] Protect Against Hackers and MalwareStoring your data on a cloud system provides added an added layer of protection from hackers and data loss.

[3] Save MoneyCloud storage is not only safe and secure, it's also cost-effective. There's no need to spend money on an entire server or storage array that you won't be using to its full capacity.

[4] It's Easier to Share and Access FilesCloud storage allows you to work much more efficiently.

[5] It's OrganizedYou can control what information is stored and how. While it is possible to simply upload everything you have, you don't need to.

III. APPROACH OF SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

Step 1: Login to the system.

Step 2: Select the data, to encrypt the data.

Step 3: Select the key to encrypt.

Step 4: Generate the signature.

Step 5: Encrypt the data.

Step 6: Upload encrypted data to the cloud.

IV. DESIGN METHODOLOGY OF SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

There are two main categories of encryptions used in cryptography to achieve data confidentiality, integrity, availability, authentication. There are symmetric and asymmetric encryption Algorithms. In Symmetric - AES, Blowfish and In Asymmetric -ECC, RSA.

1. Advanced Encryption Standard (AES):

This algorithm has been approved by NIST in the late 2000 as a replacement for DES algorithm. [7] 128 bit Advanced Encryption Standard (AES) is used for increase data security and confidentiality. In this proposed approach data is encrypted using AES and then uploaded on a cloud.

2. BLOWFISH:

Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. It is a very well-known fast secret key cryptography, with a block size of 64 bits and a variable key length ranging from 32 bits to 448 bits.[2]

3. ECC:

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. Elliptic Curve Cryptography scheme as a secure tool to model a Secured platform for the Cloud Application.[8]

4. RSA

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key (asymmetric) cryptographic methods. Since there is no efficient way to factor very large (100-200 digit) numbers, the algorithm capitalizes on the fact.[9]

V. CONCLUSION

This paper conducts a comparatives analysis of paper on secure file storage on cloud using hybrid cryptography. The main aim of this system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security are solved using cryptography and steganography techniques. Cryptography and Steganography techniques are helping to solve cloud storage security issues. Data

security is achieved. RSA, ECC and Blowfish algorithm provides Block wise data security. Less time is used for the encryption and decryption process using multithreading technique. With the help of the proposed security mechanism, we have accomplished better data integrity, high security, low delay, authentication, and confidentiality.

VI. FUTURE SCOPE

Secure File storage on Cloud has a better future as the increase in adoption of cloud have increased the security concerns of the cloud too.

In a cloud condition, progressively numbers of individuals are getting to the web server locally or all-inclusive to share the touchy information.

The proposed half and half encryption strategy is useful to improve the security for electronic exchanges in future.

In the future we can add public key cryptography to avoid any attacks during the transmission of the data from the client to the server.

VII. REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing#History
[2] Bala, Bindu, Lovejeet Kamboj, and Pawan Luthra. "SECURE FILE STORAGE IN CLOUD COMPUTING USING HYBRID CRYPTOGRAPHY ALGORITHM." International Journal of Advanced Research in Computer Science 9, no. 2 (2018).
[3] http://mp3.about.com/od/glossary/g/Cloud-Storage-Definition-What-Is-Cloud-Storage.html
[4] Jacob R. Lorch, David Molnar, Helen J. Wang, and Li Zhuang,' Enabling Security in Cloud Storage SLAs with CloudProof', Microsoft Research.
[5] Enabling Security in Cloud Storage SLAs with CloudProof. Cloud security still the biggest concern/hurdle for google, microsoft, verizon.
[6] https://www.veritas.com/blogs/why-cloud-storage-security-is-so-important
[7] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
[8] Sherif El-etriby, Emam M. Mohamad, Hatem S. Abdulkader, Modern Encryption Techniques for Cloud Computing,IEEE, ICCCI,pages 800-805
[9] Kanatt, S., Talwar, P., & Jadhav, A. (2020). Review of Secure File Storage on Cloud using Hybrid Cryptography. Int. J. Eng. Res, 9, 16-20.