International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Online Automatic Space Management and File Storage on Cloud using Hybrid Cryptography

Prerana Shendre[1], Srushti Patekar[2], Aachal Thakare[2], Gauri Ningot[2], Prof. Nupoor Yawale[3]

[1]Student, Computer Science & Engineering Department, PRMIT&R, Badnera.
[2]Student, Computer Science & Engineering Department, PRMIT&R, Badnera.
[3]Assistant Professor, Computer Science & Engineering Department, PRMIT&R, Badnera.

Abstract – In this paper, a cloud application is implemented for the corporate sector to store, share and upload documents. This application makes it easier for the employees to operate documents/files present on the cloud server/database. This paper will have solutions to upload and download documents, store documents on the server, also to view documents shared by other users and to view file details which are on the server. When the user uploads a document, it will be automatically encrypted using the hybrid algorithm. The user (employee) will be able to access shared documents as well as download them in the decrypted form using a secret key received from the registered email ID. In this cloud application, an automatic space manager will be used to track various actions related to a document, such as how many times the document is being downloaded and shared. This will help find unused files and move them on the backup server. In case the unused file's demand suddenly increases, then the file will be moved from the backup server to the main cloud server using automatic space manager.

***Key-Words*:** Cloud Computing, Hybrid Cryptography, Encryption Algorithms, Space Management, Cloud Storage.

1. INTRODUCTION:

Automatic Space management is one of the major task of cloud computing. Applying security to the files uploaded on cloud server is one of the major task of hybrid cryptography. Research work focuses on automatic space management on cloud and redirecting unused files to backup server and hybrid cryptography to prevent data accessibility by an unauthorized individual. Almost all type of data including image, video, audio, files, etc can be included. Along with this all types of cryptography algorithms including DES, AES, blowfish, ECC, RSA, SHA, etc can be used. Whereas in this research work, more emphasis is given on blowfish and ECC. In this research work, a local cloud server for corporate sector will be designed and developed comprising a cryptography-based approach for managing data.

The term "hybrid cryptography" refers to the integration of two cryptographic techniques: asymmetric encryption and symmetric encryption. If we can use multiple algorithms of different types to increase the encryption's power, we can integrate the speed and strength of the two algorithms. This method is used to assure safe cloud storage systems. Technologies used in application are Java, Eclipse Software, Apache Tomcat Server, MySQL database, JSP, Bootstrap, JavaScript, MVC, python. In research, there are four modules including Cloud Admin, Company Admin, Branch Manager and Employee.

2. PROBLEM STATEMENT:

Several cloud servers are accepting the files shared by multiple users including employees, individuals, businesses, technology, companies, etc. When these files are stored for longer time without even a single entity accessing it an issue is created related to amount of storage space. Due to large space required by files, if some files are not accessed for some defined period of time, they will use unnecessary storage space. Due to which Automatic Space management is one of the major tasks of cloud computing. Applying security to the files uploaded on cloud server is one of the major task of hybrid cryptography.

3. PROJECT OBJECTIVES:

1) To develop an online cloud-based storage system.

2) To implement automatic space management to track various actions related to documents.

3) To implement hybrid cryptography for document security.

4. RELATED WORK:

1." Secure Data Storage in Cloud Computing" by Bindu B. S., & Yadaiah, B., published in the International Journal of Research in Computer Science. This paper proposes a hybrid cryptography-based approach for secure data storage in cloud computing environments.

2." A survey on secure storage in cloud computing" by Rajathi, A., & Saravanan, N, published in the Indian Journal of Science and technology in 2013. This paper provides a comprehensive review of various hybrid cryptography techniques used for cloud storage security.

3. M. S. Abbas, S. S. Mahdi and S. A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography," 2020 published in the International Conference on Computer Science and Software Engineering (CSASE), 2020, doi: 10.1109/CSASE48920.2020.9142072.

4."Ensure Data Security in Cloud Storage" by C. Jian-quan, H. Du, X. Zhang, Y. Lin and L. Zeng, published in The Quality of Higher Education, vol. 10, in 2011. This paper proposes a hybrid cryptography-based approach for secure cloud storage, which uses a combination of AES, RSA, and MD5 algorithms.

5."A hybrid cryptography technique for data storage on cloud computing" by A. Bermani, T. Murshedi and Z. Abod, published in the Journal of Discrete Mathematical Sciences and Cryptography, vol. 24, no. 6, pp. 1613-1624, 2021. Available: Link. This paper presents a hybrid cryptography-based data storage for cloud computing. The system uses a combination of symmetric and asymmetric encryption techniques for enhanced security and reliability.

5. METHODOLOGY:

5.1 ALGORITHM'S USED:

1) Blowfish Algorithm:

Blowfish operates on 64-bit blocks of data, and supports variable-length key sizes of up to 448 bits. It uses a Feistel network structure, which involves splitting the input block into two halves and applying a series of substitutions and permutations on each half.

The key schedule of Blowfish is used to generate a series of subkeys that are used in the encryption and decryption process. The subkeys are generated by applying the Blowfish encryption algorithm to a series of incrementing values called "pi" and "sigma".

Blowfish is considered to be a secure algorithm, and has not been compromised in any significant way since its inception. However, it has been largely replaced by the Advanced Encryption Standard (AES) in modern cryptographic applications, due to its larger block size and higher performance on modern hardware.

2) Elliptic Curve Cryptography (ECC):

ECC (Elliptic Curve Cryptography) is a safe and efficient method of encrypting data and ensuring reliable network communication. A type of public key cryptography that uses its properties to generate a pair of keys for secure communication and data encryption is elliptic curve cryptography (ECC). ECC utilizes elliptic curve properties to generate a pair of keys used to create secure communication.

The ECC equation is

$$P = k * G$$

Where,

P is a point on the elliptic curve

G is a fixed point on the curve known as the generator point

This finds an integer value of k. Also, it is based on ECDLP. The private key generates the public key. This public key encrypts data that can only be decrypted using the private key. The private key is kept secure and never shared, while the public key can be freely distributed to anyone who needs it.

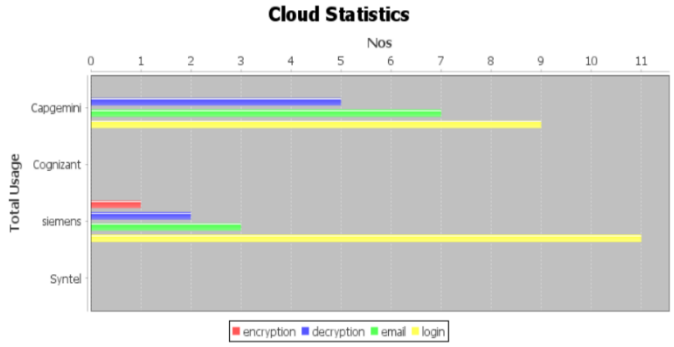
Additionally, ECC provides better resistance to attacks than other algorithms, such as RSA. Furthermore, ECC has the advantage of utilizing smaller key sizes to provide the same level of security as RSA with larger key sizes. Furthermore, ECC keys are extremely difficult to crack, making them more secure than other algorithms.

6. RESULTS:

6.1 Charts and Bar Graphs:

1) Monthly Total Cloud Usage of Clients which seen by Cloud Admin:

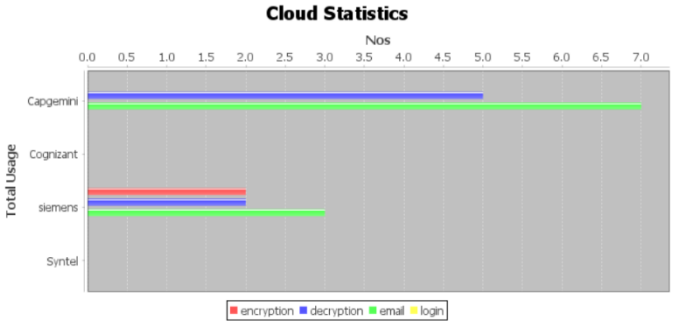
Client Name	Encryption	Decryption	Email	Login	Total
Capgemini	0	5	7	9	21
Cognizant	0	0	0	0	0
siemens	1	2	3	11	17
Syntel	0	0	0	0	0



2) Cloud Rent Report of Clients seen by Cloud Admin:

Cloud Rent Report for 4/2023

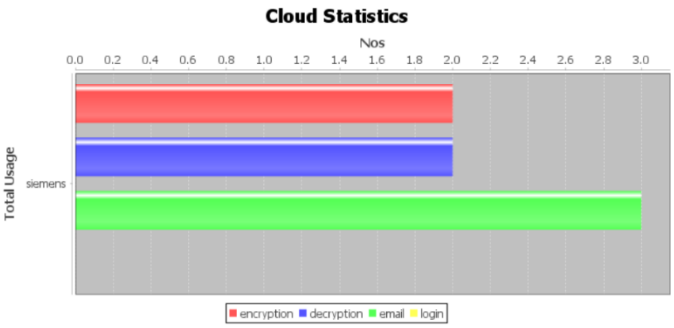
Company Name		Encryption	Decryption	Email	Login	Total Rent
Capgemini	Usage	0	5	7	9	21
	Rates	Rs. 1.0	Rs. 1.0	Rs. 1.0	Rs. 0.0	Rs. 3.0
	Rents	**Rs. 0.0**	**Rs. 5.0**	**Rs. 7.0**	**Rs. 0.0**	**Rs. 12.0**
Cognizant	Usage	0	0	0	0	0
	Rates	Rs. 1.0	Rs. 1.0	Rs. 1.0	Rs. 0.0	Rs. 3.0
	Rents	**Rs. 0.0**	**Rs. 0.0**	**Rs. 0.0**	**Rs. 0.0**	**Rs. 0.0**
siemens	Usage	2	2	3	14	21
	Rates	Rs. 1.0	Rs. 1.0	Rs. 1.0	Rs. 0.0	Rs. 3.0
	Rents	**Rs. 2.0**	**Rs. 2.0**	**Rs. 3.0**	**Rs. 0.0**	**Rs. 7.0**
Syntel	Usage	0	0	0	0	0
	Rates	Rs. 1.0	Rs. 1.0	Rs. 1.0	Rs. 0.0	Rs. 3.0
	Rents	**Rs. 0.0**	**Rs. 0.0**	**Rs. 0.0**	**Rs. 0.0**	**Rs. 0.0**



3) Payment Summary of particular company:

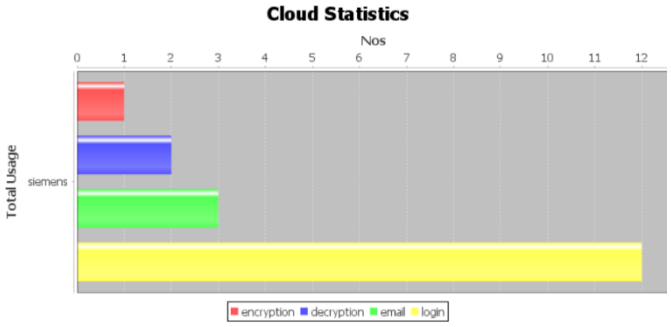
Payment History Customer Name : siemens for 2023

Months	encryption	decryption	email	login	Total Rent	Status	Payment Date
April	2.0	2.0	3.0	0.0	7.0	pending	NA



4) Total Cloud Usage of particular company seen by Company Admin:

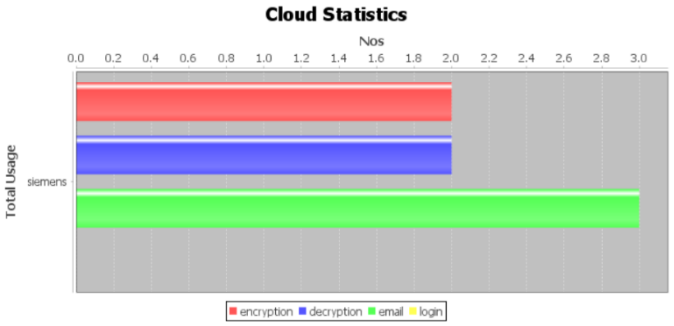
Client Name	Encryption	Decryption	Email	Login	Total
siemens	1	2	3	12	18



5) Monthly Cloud Rent Report seen by Company Admin:

Cloud Rent Report for 4/2023

Company Name		Encryption	Decryption	Email	Login	Total Rent
siemens	Usage	2	2	3	16	23
	Rates	Rs. 1.0	Rs. 1.0	Rs. 1.0	Rs. 0.0	Rs. 3.0
	Rents	**Rs. 2.0**	**Rs. 2.0**	**Rs. 3.0**	**Rs. 0.0**	**Rs. 7.0**



7. CONCLUSION:

Cloud computing has become a pivotal technology in the field of information technology, enabling users to access and store data and applications remotely through the internet. However, as the amount of data stored in the cloud continues to grow exponentially, issues such as storage space management and data security have emerged as significant concerns. This paper seeks to address these challenges by proposing an automatic space management system and implementing hybrid cryptography on a local cloud server. The automatic space management system aims to optimize storage space by automatically redirecting files that have not been accessed for more than 90 days to a backend server. This application contributes to the field of cloud computing by addressing important issues related to storage space management and data security. The automatic space management system helps optimize storage space and reducing unnecessary consumption.

The use of hybrid cryptography enhances the security of data in the cloud, safeguarding it from unauthorized access and ensuring confidentiality and integrity. The cloud statistics bar graph consist of usage of cloud services of various companies like cognizant, capgemini, etc. Whereas the cloud rent report consist of encryption, decryption, email, login and total rent. With corresponding rate as 1rs, 1rs, 1rs, 0rs, 3rs respectively.

REFERENCES

[1] Bindu B. S., & Yadaiah, B., Secure Data Storage in Cloud Computing, International Journal of Research in Computer Science, pp. 63-73.

[2] Rajathi, A., & Saravanan, N, A survey on secure storage in cloud computing, Indian Journal of Science and technology in 2013, pp. 4396-4401.

[3] M. S. Abbas, S. S. Mahdi and S. A. Hussien, Security Improvement of Cloud Data Using Hybrid Cryptography, International Conference on Computer Science and Software Engineering (CSASE), pp. 123-127.

[4] C. Jian-quan, H. Du, X. Zhang, Y. Lin and L. Zeng, Ensure Data Security in Cloud Storage, The Quality of Higher Education, pp. 284-287.

[5] A. Bermani, T. Murshedi and Z. Abod, A hybrid cryptography technique for data storage on cloud computing, Journal of Discrete Mathematical Sciences and Cryptography, pp. 1613-1624.

[6] U. Kumar and M. Prakash, A Hybrid Encryption Algorithm for Secure Data Storage on Cloud, International Journal of Creative Research Thoughts (IJCRT), pp. 2320-2882.

[7] Christina Thomas, Gnana Sheela K, Saranya P Krishnan, A Survey on Various Algorithms Used for Elliptic Curve Cryptography, pp. 7296-7301.

[8] Harmanbir kaur, Meenakshi Sharma, Security Enhancement for Cloud Storage Systems, pp. 7359-7362.

8. BIOGRAPHIS:

Prerana M. Shendre, Student at PRMIT&R, Badnera-Amravati, Maharashtra, India. Her Research area includes Cloud Computing and Cybersecurity. Contact her at preranashendre@gmail.com

Srushti A. Patekar, Student at PRMIT&R, Badnera-Amravati, Maharashtra, India. Her Research area includes Cloud Computing and Cybersecurity. Contact her at patekarsrushti92@gmail.com

Aachal G. Thakare, Student at PRMIT&R, Badnera-Amravati, Maharashtra, India. Her Research area includes Cloud Computing and Cybersecurity. Contact her at aachalthakare01@gmail.com

Gauri S. Ningot, Student at PRMIT&R, Badnera-Amravati, Maharashtra, India. Her Research area includes Cloud Computing and Cybersecurity. Contact her at gauri18ningot@gmail.com

Nupoor M. Yawale working as an assistant professor at PRMIT&R, Badnera-Amravati, Maharashtra, India. Her Research area includes Cloud Computing, Image processing and Machine Learning. Contact her at nupooryawale2021@gmail.com