Secure storage in the Cloud using Hybrid Cryptography & 2FA

Aditi Maulekhi[1], Khusharth A. Patani[2], Viral Sangani[3], Gurveen Singh[4], Prof. Nikhilkumar Shardoor[5]

[1-5]*Department of CSE, MIT ADT University, Pune, India*

***Abstract*—** In today's world cloud computing is used almost everywhere like personal usage, industry, universities and even in the military to store a large amount of data. Data can be retrieved from the cloud at the request of the user. To store data on the cloud a user has to face many issues one of which is security. To provide the solution to these issues there are many ways. Cryptography techniques are more popular now a day's for data security which mostly uses some encryption algorithm to protect the data. But using only a single algorithm is not secure enough to protect the data. So in the proposed system, a new security mechanism is designed using a hybrid cryptography algorithm and two-factor Authentication. Here, AES, Blowfish, and RSA algorithms are used to provide block-wise security to data. Key information contains which part of the file is encrypted using which algorithm and key. The file is divided into three parts and then on each part, a different encryption algorithm is used. All the encryption happens in parallel using multithreading to improve the performance of the algorithm. For file decryption purposes reverse process of encryption is applied. With hybrid cryptography, a two-factor authentication system is also added to increase the security of the system.

Keywords- AES, RSA, Blowfish, Encryption, Integrity, Data Security, Two Factor Authentication, Hybrid Cryptography.

I. INTRODUCTION

In today's world, more people are getting connected to the internet due to which the importance of data security is also increasing. We are surrounded by different IoT devices like smart home devices and electronic devices like smartphones, laptops, etc. which are consuming our data day by data. But why is data security important? As data can be used for the growth and success of a business it has become a valuable business asset. The security of the data, therefore, must be a priority and it needs to be protected from unauthorized access to prevent it from being tampered with, destroyed, or disclosed.

Security can be breached in a number of ways, for example, system failure, theft, inappropriate usage, or unauthorized access. Everything that is connected to the internet is at a risk of getting exploited. Therefore, to improve the security of our data we can use different techniques like using encryption and decryption for storing and retrieving our data. Use of features like Two Factor Authentication should be enabled in all your applications. People should be educated more on this topic as it is important to understand where your vulnerabilities are and to protect yourself accordingly.

The cryptography technique is divided into symmetric-key cryptography and public-key cryptography. This technique uses keys to translate data into unreadable form. So only an authorized person can access data from the cloud server. In this paper, a solution is proposed to improve the security of traditional cloud storage system by using a hybrid cryptographic algorithm for encrypting and decrypting files on the server. Using hybrid cryptography, the complexity of the encryption algorithm can be increased. This hybrid approach of using multiple encryption algorithms with two factor authentication makes the remote server more secure where the important data is stored which in the end will help different cloud providers to gain more trust of their users towards their system.

In this paper Section 1 includes Introduction, Section 2 includes existing system, Section 3 contains proposed system, Section 4 contains Mathematical Model, Section 5 contains implementation, Section 6 contains Conclusion and Section 7 contains Future Scope of our system.

II. EXISTING SYSTEM

In 2016, Punam V. Maitri and Aruna Verma proposed a paper on Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm where the author has proposed solutions to issues faced by users to store data in the cloud. The proposed system is using AES, blowfish, RC6, and BRA algorithms to provide high level of security to data, and the LSB steganography technique is used for key information security. Here the file is divided into 8 parts and each part is encrypted using a separate algorithm simultaneously.

In 2019, Lalit Kumar and Neelendra Badal made a paper on A Review on Hybrid Encryption in Cloud Computing where they have majorly focussed on two approaches i.e. AES and FHE. Paper tells how the hybrid approach helps the user to keep data more redundant and secure in comparison to some other.

In 2019, Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam proposed a new security mechanism that uses a combination of multiple cryptographic algorithms of a symmetric key (3DES, RC6 and AES) and steganography to provide security to data.

In 2019, Shweta Kaushik; Ashish Patel have proposed a hybrid approach using symmetric encryption to provide more security for the user's data. This use of a hybrid approach makes data more secure and protect it from any malicious activity attended by an intruder. The use of symmetric encryption increases the processing ability and brute force also is impossible in this approach.

TABULAR REPRESENTATION OF THE LITERATURE SURVEY

CITATION	METHODOLOGY	FEATURES	CHALLENGES
2019 [1]	Hybrid Cryptography	Security of owner's data and protects it from malicious activities by an intruder.	With the advancements in technology more advanced symmetric or asymmetric cryptographic algorithms can be used to provide more data security.
2019 [2]	Cloud computing	Making the client's privacy by storing client data on a single cloud, using AES, DES, and RC2 algorithm.	The scheme doesn't have the feature of group sharing of data among a set of people in the shared data section.
2016[3]	Cloud computing	The scheme ensures data security while transferring, sharing, and storing in the data centers using data classification, Hashed Message Authentication, and Indexing.	The algorithm used has no mathematical proof.
2016[4]	Cloud Computing	Data owner (DO) externalizes the encoded data at cloud server to make masked from invader and grants access to an only legitimate user with the corresponding decipher key to decode it and obtain the original data.	The scheme uses CSP, a third party for storing the data and delivery of data to the authenticated user.
2017[5]	Cloud Computing, Hybrid Cryptography	Data security and maintaining the owner's privacy, confidentiality, and integrity.	Only theoretical explanations given lacks practical implementation.
2018[6]	Hybrid Cryptography, Cloud computing	Less encryption and decryption time as compared to other symmetric technique like Blowfish and AES	Asymmetric encryption techniques are more secure and fast.
2018 [7]	Attribute-based encryption and byte rotation encryption	Increased privacy of data in a peer to peer network exchange by adding BRE and ABE algorithm	The system is not heterogeneous so the user cannot work on any platform/ machine.
2016 [8]	Cloud computing	symmetric-key cryptography algorithm and steganography are used to provide block-wise security to data.	AES provides more security than symmetric algorithms.
2015 [9]	Hybrid cryptography, digital signature, and Diffie Hellman key exchange	The algorithm is designed as a combination of AES and DES and used of Diffie Hellman key exchange enhances the security of data.	-
2018 [10]	Cloud computing and cryptography	Improved privacy for inter-cloud data sharing.	Homomorphic encryption
2013 [11]	Hybrid cryptography	Combination of substitution and transportation	The use of traditional cryptographic algorithms makes it less secure.
2020 [12]	Hybrid cryptography, cloud computing	Providing security to big data before storing it in multi-cloud.	-

III. PROPOSED SYSTEM

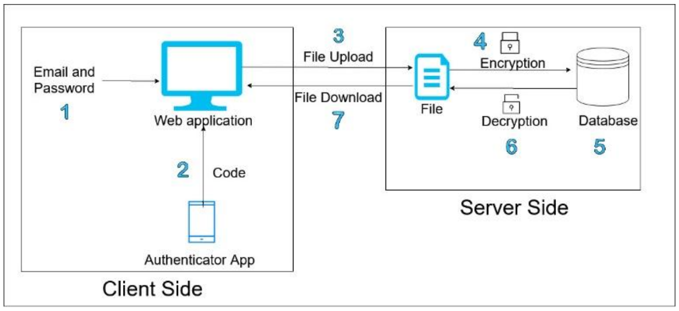


Figure 1: Client-server architecture

The proposed system is based upon the client-server architecture and the system can be divided into two parts as follows:

- Client-side which includes a web application and a two-factor authenticator app.
- Server-side, where hybrid encryption and decryption algorithm will be used and uploaded files, will be stored.

The client-side consists of a web application and an authenticator app. To access the web application the user first enters the registered email ID and password after which the user is asked for a code which is generated in our authenticator app Using this code through the authenticator app two-factor authentication in the web application is enabled. After entering all the details, the user gets access to the dashboard using which files can be uploaded and downloaded.

On the server-side when a file is uploaded, the server applies the hybrid encryption algorithm to encrypt the uploaded file and then save it in the database. When a file is requested for download the server takes the encrypted file from the database, decrypts it, and then sends it back to the requested client.

IV. MATHEMATICAL MODEL

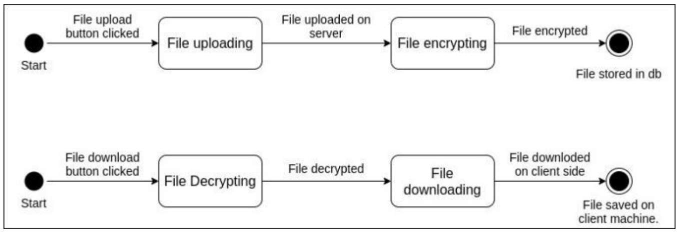


Figure 5: State transition diagram for file upload and download

- Let K1 and K2 be Public key and Private Key of RSA Algorithm respectively.
- Let K3 be Key for AES Algorithm.
- Let K4 and K5 be Public key and Private Key of BlowFish Algorithm respectively.
- F is the File uploaded by the user. F can be JPG, JPEG, MP3, MP4, PNG, TXT.
- F is split into 3 equal parts - F1, F2, F3.
- F1e, F2e, F3e is the encrypted format of F1, F2, and F3.

Step 1: Convert the uploaded file to binary data and split the uploaded file into F1, F2, and F3:

F = Split(F1, F2, F3)

Step 2: Upon applying RSA on F1 with K1 as Public Key, F1e is obtained and can be stored in the File system.

F1e = RSA(F1, K1)

Step 3: Applying AES on F2 with K3 as Key, F2e is obtained and stored in the File system.

F2e = AES(F2, K3)

Step 4: F3e is obtained by applying BlowFish on F3 with K4 as Public key after which F3e can be store in the File system.

F3e = BlowFish(F3, K4)

Step 5: To decrypt, each file (F1e, F2e, F3e) has to decrypt individually and merged together.

Step 6: To decrypt F1e using K2 as the Private key of the RSA algorithm, origin F1 can be obtained.

Step 7: F2 can be obtained by decrypting F2e with an AES key, i.e. K3.

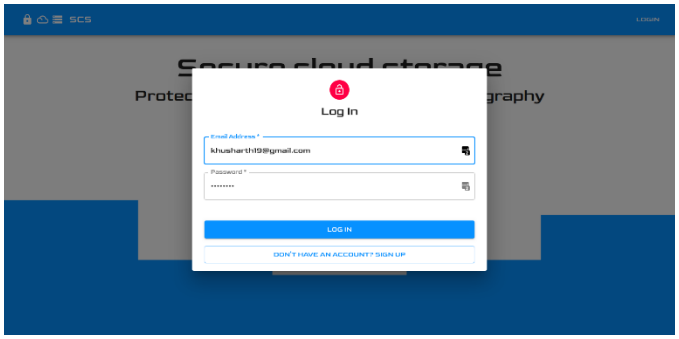
Step 8: To get the F3, F3e is decrypted with the Private key of the Blowfish algorithm i.e. K5.

Step 9: Original file F is obtained by merging F1, F2, F3.

F = Merge (F1, F2, F3)

V. IMPLEMENTATION

A user first has to register on the web application to create an account and once the account is created the user also gets access to the authenticator app in which the two-factor authentication code is generated every 30 seconds.

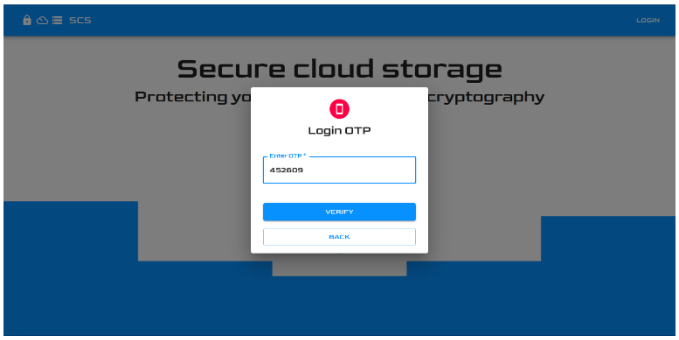


Email Address * khusharth19@gmail.com

Password * ·········

Figure 2: Login Screen

In the web application, the authentication system is implemented using firebase. When a user tries to login the firebase API checks if the user exists and if it does then returns a JWT token for that particular user.



Enter OTP * 452609

Figure 3: OTP Verification Screen

On the next step, the user has to enter the code from the authenticator app which is then sent to the secure cloud storage API server with the JWT token from the previous step. Once the code is verified the user gets access to the dashboard.

In the dashboard, the user has the option to either upload or download files. If a user selects to upload a file then the file is uploaded to the secure cloud storage server. Once the file is received on the server the file gets converted to binary code and gets divided into 3 equal parts. Then the hybrid encryption algorithm is applied which consists of 3 different algorithms which are AES, RSA, and Blowfish. The encryption algorithms are applied parallelly to all 3 equal parts so as to reduce the algorithm time. After encrypting the file is saved in the database.

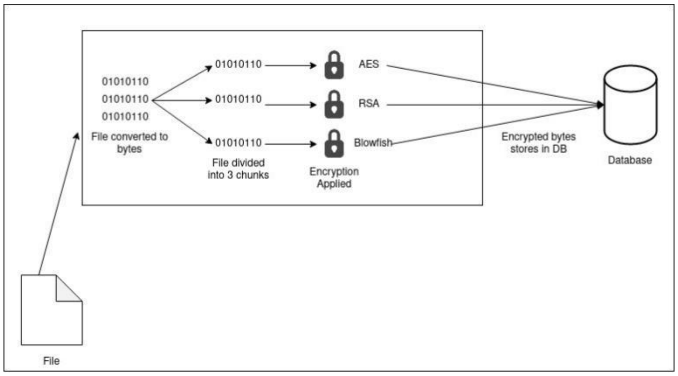


Figure 4: Hybrid Encryption Algorithm

When a user requests a file for download the 3 parts of the file are retrieved from the database on the server and then the decryption algorithm is applied. Once the binary code gets decrypted, it is joined back to convert the file back to its original form. After that, the file is sent back to the requested client and the user is able to download this file.

VI. CONCLUSION

Using the web application, the authenticator app, and the hybrid algorithm a secure cloud storage system is formed in which due to the use of two-factor authentication the security of the system is increased, and by using the hybrid algorithm the security of file storage is improved for encryption and decryption of files.

VII. FUTURE SCOPE

In the current scope, the algorithm is responsible only for encryption and decryption but due to the use of multiple algorithms the time taken to encrypt and decrypt a file could be large so this algorithm can be further optimized to reduce the number of algorithms used for encryption and decryption depending upon the size of the file uploaded or downloaded.

REFERENCES

[1] P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 1635-1638, DOI: 10.1109/WiSPNET.2016.7566416.

[2] L. Kumar and N. Badal, "A Review on Hybrid Encryption in Cloud Computing," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6, DOI: 10.1109/IoT-SIU.2019.8777503.

[3] Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam, "Secure File Storage on Cloud using Hybrid Cryptography", International Journal of Computer Sciences and Engineering, Vol.7, Issue.1, pp.587-591, 2019.

[4] S. Kaushik and A. Patel, "Secure Cloud Data Using Hybrid Cryptographic Scheme," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6, DOI: 10.1109/IoT-SIU.2019.8777592.

[5] Akshita Bhandari, Ashutosh Gupta, Debasis Das. "A framework for data security and storage in Cloud Computing", 2016 International Conference Techniques in Information and Communication Technologies (ICCTICT), 2016.

[6] Shweta Kaushik, Charu Gandhi. "Cloud data security with hybrid symmetric encryption", 2016 International Conference Techniques in Information and Communication Technologies (ICCTICT), 2016.

[7] P. Chinnasamy, P. Deepalakshmi, "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography", ICICCT, 2018

[8] P. more, S. Chandugade, S. M. S. Rafiq, Prof. P. Pise, "Hybrid Encryption Techniques for Secure Sharing sensitive data for banking system over Cloud", ICACCT, 2018.

[9] P. Kanchan, "Use of Digital Signature with Diffie Hellman Key Exchange and Hybrid Cryptographic algorithm to Enhance Data Security in Cloud Computing", Volume 5, Issue 6, ISSN 2250- 3153, pp 1-4, June 2015

[10] Kartit, Z., Azougaghe, A., Kamal Idrissi, H., El Marraki, M., Hedabou, M., Belkasmi, M., & Kartit, A., "Applying Encryption Algorithm for Data Security in Cloud Storage", Advances in Ubiquitous Networking, 141–154. doi:10.1007, 2016

[11] Arockiam, L., Monikandan, S.: "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering 2(8), August 2013

[12] Viswanath, G., & Krishna, P. V.," Hybrid encryption framework for securing big data storage in multi-cloud environment", Evolutionary Intelligence. doi:10.1007, 2020

[13] Jouini M, Rabai LBA, "A security framework for secure cloud computing environments" In Cloud security: concepts, methodologies, tools, and applications. IGI Global, pp. 249–263, 2019

[14] Du M, Wang Q, He M, Weng J, "Privacy-preserving indexing and query processing for secure dynamic cloud storage", IEEE Trans Inf Forensics Secur 13(9):2320–2332, 2018

[15] Nagendra, M., Sekhar, "M.C.: Performance Improvement of Advanced Encryption Algorithm using Parallel Imputation.", International Journal of Software Engineering and Its Applications 8(2), 287–296, 2014

[16] Zhang, X., Wu, N., Yan, G., et al.: Hardware Implementation of Compact AES S-box. IAENG International Journal of Computer Science 42(2), 2015

[17] AbdElminaam, D.S., "Improving the security of cloud computing by building new hybrid cryptography algorithms.", International Journal of Electronics and Information Engineering, 8(1), pp.40-48, 2018

[18] D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," *International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS)*, Vellore, pp. 1-5, DOI: 10.1109/ICMDCS.2017.8211728., 2017

[19] Taha, A.A., AbdElminaam, D.S., and Hosny, K.M., NHCA: Developing New Hybrid Cryptography Algorithm for Cloud Computing Environment. (IJACSA) International Journal of Advanced Computer Science and Applications, 8(11), 2017

[20] Bala, B., Kamboj, L. and Luthra, P., SECURE FILE STORAGE IN CLOUD COMPUTING USING HYBRID CRYPTOGRAPHY ALGORITHM. International Journal of Advanced Research in Computer Science, 9(2), 2018