Migration Letters

Volume: 21, No: S5 (2024), pp. 493-508

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Design Of An Effective Hybrid Cryptographic Technique For Information Security In Cloud Computing

Anjana[1], Dr.Ajit Singh[2]

Abstract

The cloud computing technology of the future offers high availability, virtualization, and dynamic resource pools. Cloud computing is a technique to tackle typical computing problems, such as hardware, software, and resource availability, without the involvement of computer users. The two most significant issues with cloud computing are cloud security and cloud implementation over the network. There are lot of cryptographic algorithms existing to encrypt the data in cloud storage but with various loopholes. The proposed solution is a hybrid technique utilizing RSA, Blowfish, and MD5; it enables users to exchange data securely within a cloud environment. MD5 is currently the most prevalent symmetric cryptography algorithm. It is crucial to build a high-performance variant of MD5 to expand its wider application. The RSA as well as Blowfish encryption method is used to encrypt data when a cloud user uploads it to the cloud environment. The cloud controller can use his or her own private key to decrypt the data. Cloud computing is a tried-and-true, scalable, and effective approach for offering services. Finally, performance evaluation has been completed by contrasting the outcomes of the proposed hybrid technique with those of the existing techniques.

Keywords: *Cloud Computing, Encryption, Decryption, Cypher text, RSA, Blowfish and MD5*

1. INTRODUCTION

Computer technology uses cloud computing. It has become an IT buzzword in recent years. Cloud, SaaS, grid, cluster, autonomic, and utility computing are sometimes used interchangeably. Cloud services include SaaS. Cloud computing relies on grid and cluster computing [1]. Cloud computing uses several resources to provide remote services through a network. It maximizes capacity while minimizing resources. The user uses minimum hardware to its fullest. Computer is virtual computing resources. Internet users can access computational resources [2]. Applications need its programming environment. It dynamically deploys, reallocates, and monitors computer resources.

Software manages all cloud computing resources. It analyses historical and present data to improve accuracy and give smarter services to customers and enterprises. Users do not buy servers, software, etc. Online us[1]ers can buy computing power [8]. Grid computing and efficiency lead to cloud computing, which not need a data centres. Cloud computing expansion and management are easy. The cloud manages resources and can serve millions of people. Third parties or organizations can provide cloud hardware (hosted clouds) [3]. A cloud might be private, public, or shared by numerous companies (hybrid clouds).

2. LITERATURE REVIEW

Department of CSE & IT, Bhagat Phool Singh Mahila Vishwavidyalaya, Khanpur Kalan, Sonipat, Haryana, India.

This section describes current research accomplishments in the classification of cloud computing and cloud security challenges that support our theoretical foundation and research history.

Kanchanadevi P. et.al (2020) [4] studied that the adaptable platform of cloud computing allows for the outsourcing of data from local servers to commercial clouds. Despite the fact that cloud computing offers users a host of advantages, data leakage and privacy issues make cloud less popular. Numerous measures must be used in the cloud to secure data privacy and minimise data leakage. Although there are many different kinds of cloud environments, we focus on hybrid cloud. Hybrid clouds are simply combinations of two or more clouds. where non-critical operations are carried out in the public cloud and important operations are carried out in the private cloud. It therefore has several benefits and is essential. have put a strong emphasis on data security via a hybrid cloud encryption technique.

Rani, P. K., Sathiya et.al. (2022) [5] conducted that Cloud computing aims to centralize data processing and storage. Mobile and cloud computing may process massive volumes of data quickly, enhancing performance needs. That study employs numerous cryptographic standards, such as Attribute Based Proxy Re-Encryption, to construct a secure model with data privacy, security, integration, as well as dynamic distribution with access control in a protected environment. The ABE also uses homomorphism encryption, making data deciphering nearly impossible. Cloud computing aims to centralize data processing and storage. Mobile and cloud computing may process massive volumes of data quickly, enhancing performance needs.

Murad, S. H., et.al. (2022) [6] described that Cloud computing is a popular Internet data storage and retrieval method. Customers may not control distant servers that store sensitive data. Thus, cloud service providers and others may attack stored data. Cloud security relies on cryptography. Hybrid cryptography uses many algorithms to improve security and speed. Furthermore, examined from 2013 - 2020 hybrid cryptographic methods for cloud data security and presented each proposition's conception, strategy for implementation, restrictions, and suggested uses.

Abroshan, H. (2021) [7] examined that Cloud services have a major difficulty in cloud computing security. Data encryption in a cloud context, which uses shared resources, must not affect performance. Thus, this work presents a secure cryptographic solution for cloud computing with minimal performance impact. Cloud computing requires speed, thus sophisticated cryptography algorithms are useless. This method employs a modified Blowfish algorithm with an elliptic-curve-based methodology. Using the elliptic curve approach, Blowfish will encrypt data and keys, thereby enhancing security and performance. Digital signatures preserve data integrity.

Orobosade et.al. (2020) [8] described that the tremendous rise of sensitive cloud data has rendered it more vulnerable. Thus, the growing number of malevolent users increases vulnerability. Cloud security services are crucial due to the fact that the cloud is maintained by a third party and that cloud data as well as services are becoming more common in data centres. Users of the cloud must therefore protect their data. Describe a privacy model where ECC employs an AES key to achieve data confidentiality and cloud security, and AES is used as a first-level data encryption solution before cloud application data storage.

Taha, A. A. et.al. (2017) [9] conducted Mobile cloud computing is significant now because it is available, usable, and connects mobile to cloud computing. Cloud data is sent from mobile to cloud and vice versa via a network, ensuring data security. Encryption algorithms are needed to secure transferred data quickly and efficiently. The suggested system encrypts and decrypts mobile-to-cloud data efficiently. Shows a mobile-cloud data encryption system and provides encryption techniques. The method would assist mobile-cloud users secure their sent and received data from theft.

Table 1- Comparison of different existing encryption algorithms [23][24]

Author's Name	**Techniques**	**Findings**	**Limitations**
Hagge M [10]	**3DES**	This algorithm is simple to use, widely used, and very secure.	It is a waste of time because it is applied three times to the same data.
Zhou X [11]	**RSA**	This procedure is fast, simple, and safe.	Not able to scale. User security only works.
Chauhan A [12]	**Blow Fish**	This method is among the quickest block cyphers currently in use.	Blowfish key management is complex and cannot authenticate two users with the same key.
Sachdev A [13]	**AES**	This protects data against brute-force attacks.	Data efficiency and privacy are not prioritized.
Nicholas, K [14]	**MD5, RSA**	Get the RSA encryption algorithm, which secures the security server and client.	Less security by using OTP
Bangar and Shinde [15]	**DES, AES, Dife Hellman, digital signature, RSA**	Enhance the security of cloud	High performance may be not as critical as academia.
Gunasekaran & Lavanya [16]	**RSA & AES algorithms**	Improve cloud computing data security	After the data has been decrypted on the user end, any requests to read it will take place.
Kratit [17]	**AES & RSA Algorithm**	Secure the data and bolster defenses against harmful attacks Secure the data and bolster defenses against harmful attacks	Cloud storage solutions are not suitable for large companies.
Yugandhara [18]	**AES & HMAC**	Enable user to send data to cloud without worrying about data loss	The need for security improvements and a trustworthy authentication mechanism that can help to reduce illegal access

Salem [19]	**AES & MD5**	Increases data accessibility for the public, ensures that the data is correctly stored, increases data availability, and protects data confidentiality.	the approach for assures cloud data is redundancy

3. PROPOSED METHODOLOGY

The obstacles motivate us to create a correct, secure, and efficient approach for protecting cloud-stored data.

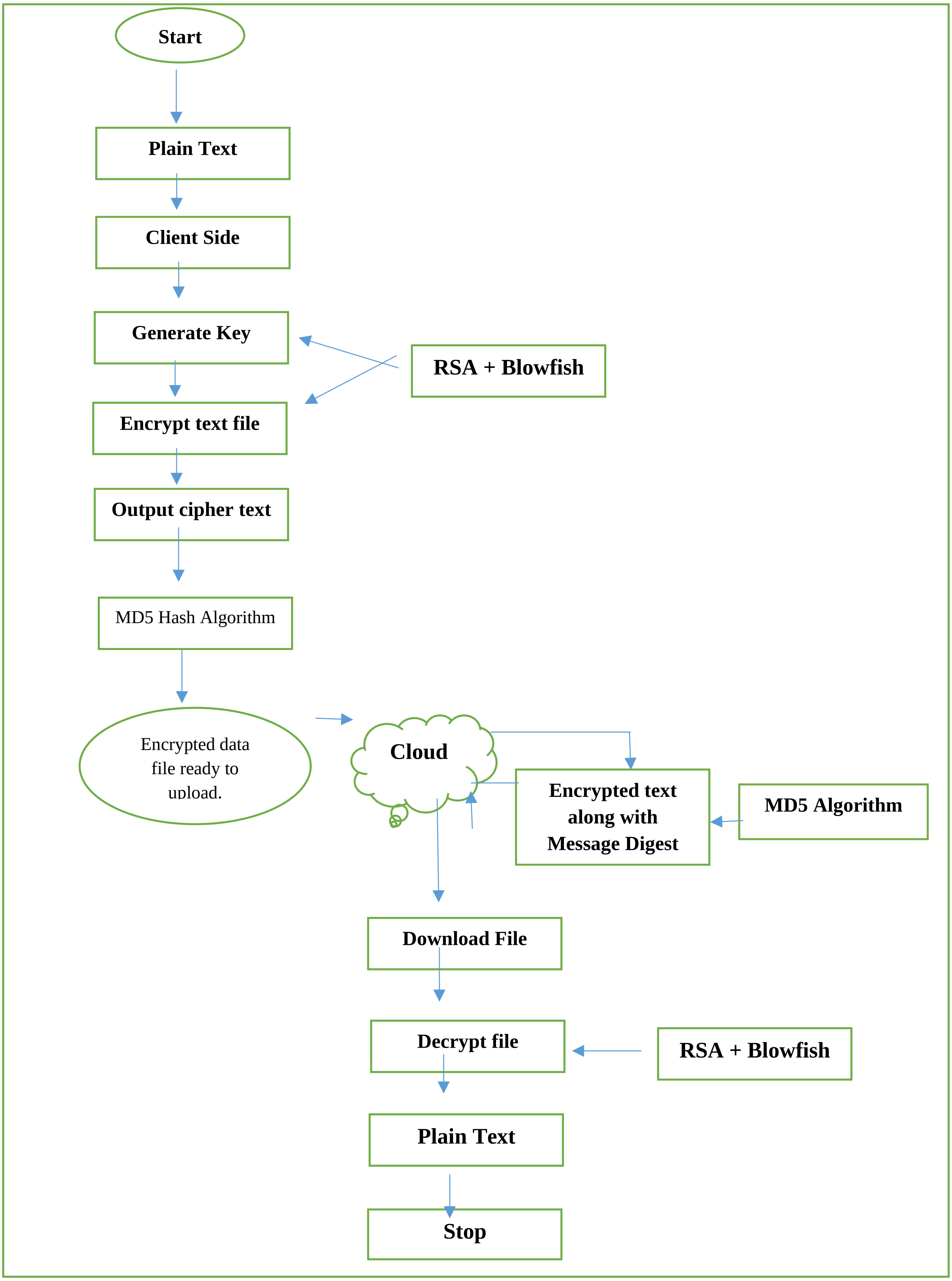

Start
Plain Text
Client Side
Generate Key
RSA + Blowfish
Encrypt text file
Output cipher text
MD5 Hash Algorithm
Encrypted data file ready to upload.
Cloud
Encrypted text along with Message Digest
MD5 Algorithm
Download File
Decrypt file
RSA + Blowfish
Plain Text
Stop

Figure 1 - Flowchart for Cloud Computing

Figure 1 flowchart proposed hybrid encryption algorithm based on RSA, Blowfish and MD5 combination. It is three step processes where file is encrypted using RSA and then Blowfish. After that to enhance the security MD5 is applied to the output which confirms the security of stored data.

- **RSA:** According to below given figure 2 represents block diagram of RSA algorithm created by Adi Shamir, Leonard Adleman, and Ron Rivest. Its foundation is positive integers. RSA encryption and decryption use modular exponential [10]. The public-key algorithm RSA uses public and private keys. Everyone can use the public key to encrypt messages. The only key that can decrypt public key-encrypted communications is the private key.

RSA Algorithm

a) Select two random prime no. p & q.

b) Calculate n=p*q.

c) Calculate Φ(n)=(p-1)*(q-1).

d) Choice at random the encryption key e, where 1<e<Φ(n) & gcd(e, Φ(n))=1.

e) Calculate d= e^{-1} mod Φ(n), To find the decryption key.

f) Public encryption key: KU={e,n}.

g) Private decryption key: KR={d,n}.

Encryption and Decryption

a) Calculate C=M^e mod n, where 0<&<n.

b) Calculate M=C^d mod n, decryption.

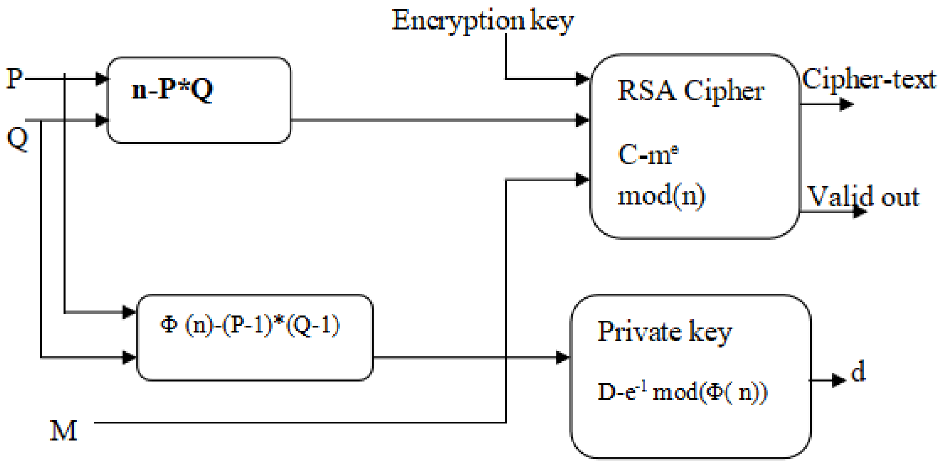


Figure 2 - Block diagram of RSA algorithm

RSA employs two exponents—e & d—where e is a public exponent as well as d is a private exponent. Let M & C be the plaintext & cypher text, respectively, before encrypting.

$C = M^e \bmod n$

And at decryption side

$M = C^d \bmod n.$

Where n is an extremely high no. generated through key creation.

File Upload

This approach consists of three components. During the initial part of the process, Clair text is encrypted with RSA. Then its output is encrypted with the blowfish algorithm in the second phase [21]. Then MD5 is applied to the output.

Our algorithm employs the subsequent functions:

Number Of Block(F): It returns the number of block in the file F.

ENC_RSA (B,K): It encrypts the block B using RSA Algorithm with key K.

ENC_Blowfish: It encrypts the block B using Blowfish Algorithm.

send_to_cloud(F'): It permits to send the encrypted file F in Cloud storage.

ENC_MD5(k): It enhance the message security by applying MD5 Algorithm

Save_in_server(K'): It permits to save K' in the server.

Algorithm: File Upload

```
Encrypt file (F) {
/* algorithm to encrypt file onto cloud storage */
/* to transform Clair text in file F into Cipher text in file F */
 /* Phase 1: Encrypt Clair text with RSA algorithm */
For B ← 1 to number of block (F) do
{
B=ENC RSA (B, K)
}
Convey to cloud (F)
/* Phase 2: Encrypt output with Blowfish algorithm */
For k ← 1 to size of (K) do
{
K= ENC Blowfish (K)
}
Save in server (K)
Phase 3: Apply the output with  MD5 algorithm
For G ← 1 to no. of block (F) do
{
K = ENC MD5(K)
}
```

Decryption: This form decrypts the file using the private key. This form also demands a list of authorized keys [22].

- **File Download:** Additionally, this method has three parts. Using the server's MD5 key, the encrypted content is translated. The algorithm uses:
  Block (F)'s no.: Returns the total no. of file F's blocks.
  DEC MD5 (B', K): Block B' is decrypted with the MD5 algorithm and key K.
  DEC Blowfish(k')

DEC RSA (k’): To decrypt k', the RSA algorithm is applied.

Algorithm: File Download

```
Decrypt file(F) {
/* formula for data downloaded from cloud storage that have been decrypted */
/* to transform the text in file F (Cipher) into the text in file F (Clair) */
/* Phase 1; decryption using the MD5 technique */
for K ← 1 to size of (K) do
{
    K= DEC MD5 (B’,k)
}
return (K)
/* Phase: 2 Blowfish algorithm is used to decrypt cypher text */
for B ← 1 is the number of block (F) do
{
    B= DEC Blowfish (B, K)
}
Phase 3; decryption using the RSA technique */
for G← 1 is the number of block (F) do
{
    return (F)= DEC RSA(k’)
}
```

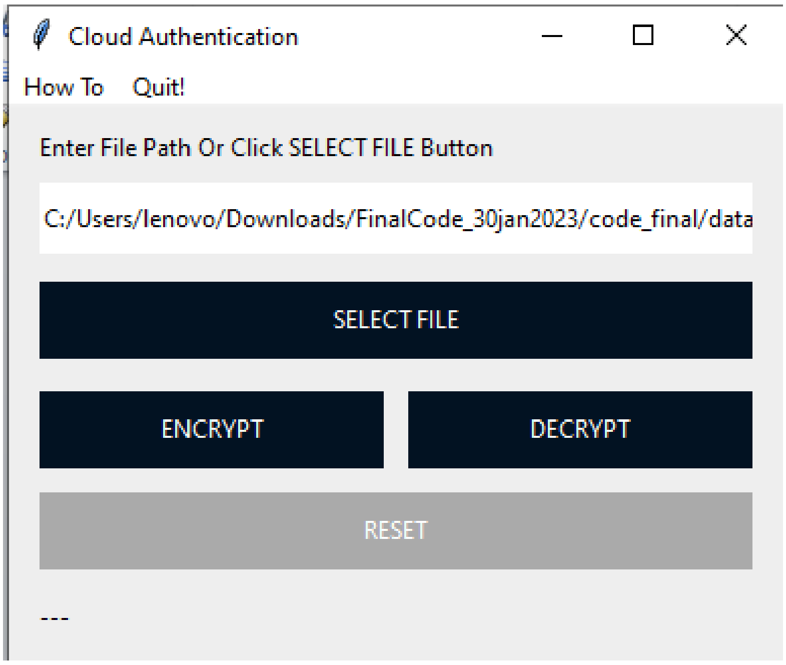
5. IMPLEMENTATION RESULT

In this part, the implementation shows how long it takes to upload and download different file sizes. The model is run on a Firebase cloud. Spyder (Python 3.9) and Anaconda are programming tools for Python. For various inputs, we test the encryption algorithm's speed, mean time, and buffer size. Speed, buffer size, and interim are defined first.

a. Meantime is the difference between the beginning and finish times of an algorithm's encryption process. If the size of the data increases, so does the time required for encryption.

b. Speed UP is a difference between the local system and the mean time cloud. If the size of the data increases, performance may decrease.

Encryption: Encrypting as well as decrypting a file in this format produces the public and private keys. The owner of the data must only submit their file and public key. The public key of the cloud server identifies the owner. Then file is encrypted using the specified private key. Figure 3 represents the User Interface of the proposed utility used for encryption and decryption.

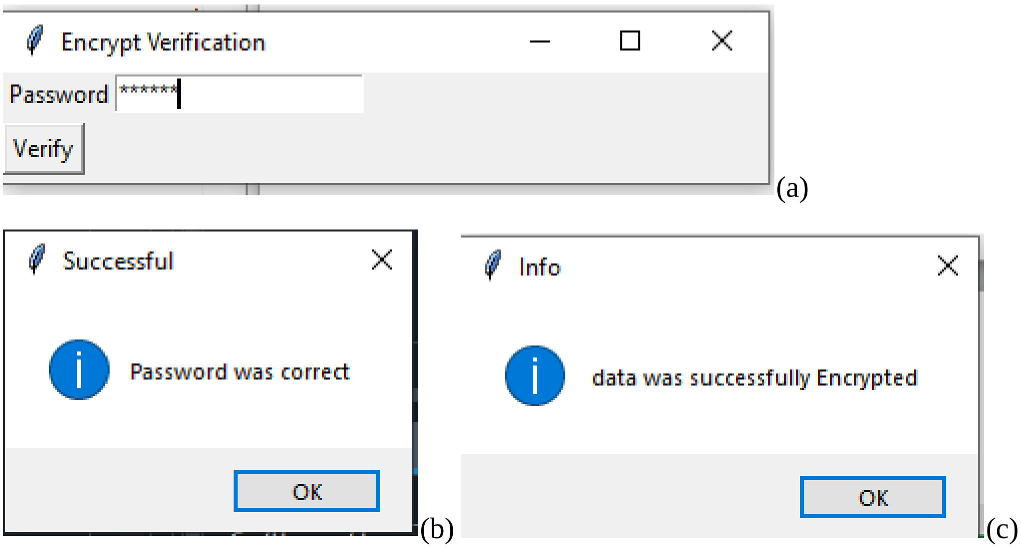


C:/Users/lenovo/Downloads/FinalCode_30jan2023/code_final/data

---

Figure 3 – Cloud Encryption Utility

Access Permission: Two different access permissions—read only and read and write only—have been set for the file that has been uploaded. After the permissions have been defined, this access authorization is recorded and the owner confirms its permissions. Figure 4 explains how the keys is entered and validated before starting the encryption process.



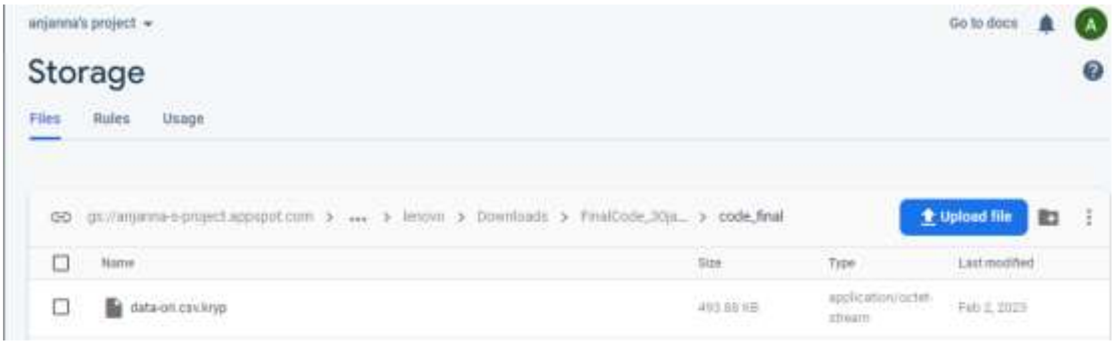
Password ******

Password was correct

data was successfully Encrypted

Figure 4 – a) Encryption Password Verification, b) Successful Message c) Successful Encryption Message

Data Uploaded On Cloud Server: After encryption the owner just uploads encrypted files to the FireBase cloud as shown in Figure 5. After uploading, the owner receives generic information about the file, including its name, size, date and time of upload, and a hash value for verification. Downloading allows the user to download the encrypted item, while Delete allows the owner to delete the submitted file.

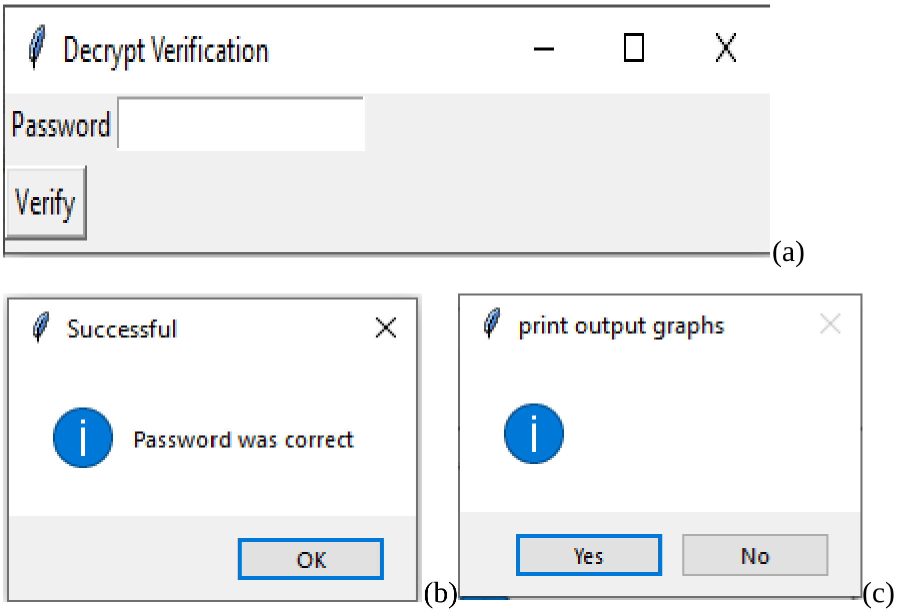

anjanna's project
Go to docs
A
Storage
Files
Rules
Usage
gs://anjanna-s-project.appspot.com > ... > lenovo > Downloads > FinalCode_30ja... > code_final
Upload file

□	Name	Size	Type	Last modified
□	data-on.csv.kryp	493.88 KB	application/octet-stream	Feb 2, 2023

Figure 5 – File uploaded on Firebase Cloud

In cloud computing, users create the application for deployment on the cloud software environment provider to compare the symmetric key algorithm. The provider of cloud-based software environments offers developers a programming-level environment with a clearly defined set of APIs. One example is Google Apps Engine, which provides a runtime environment and APIs. For Google connection, "runtime programmes are executed in the cloud and packaged."

Decryption: In Figure 6, we can see how using the private key that you provided, this form will decrypt the file. This form also requires an access list of users who have already authenticated themselves.



Password was correct

Figure 6 – a) Decryption Password Verification, b) Successful Message c) Print output graphs

At last step, utility displays the graphs for all the attributes involved like retrieval time, loss, speed, throughput etc. Table 2 shows the results on basis of retrieval time.

Table 2: Comparison of Retrieval Time between existing techniques versus Proposed Hybrid Technique

EPOCH	RSA	Blowfish	MD5	Proposed
20	76.54%	84.25%	89.5%	90%
40	82.45%	87.25%	81.48%	92.3%
60	88.52%	79.25%	81%	94.22%
80	86.55%	78.52%	85.12%	95.7%
100	87.41%	89.10%	92%	98%

Retrieval vs Epoch

Retrieval: The phrase "accuracy" refers to a statement that can be objectively checked or confirmed using existing facts and is most frequently used in situations that are clearly defined and in which it denotes "free from error or flaw." In this instance, the statement's objective meaning is so obvious that neither it nor the evidence provided to support it are subject to debate. Each statement in a sentence must comply with this condition. Additionally, divide the total number of classifications by the no. of correct classifications.

Epoch: An epoch in cloud computing is a date and time that a computer uses to calculate system time. The majority of computers calculate time as a number that represents the seconds subtracted from a given arbitrary date and time.

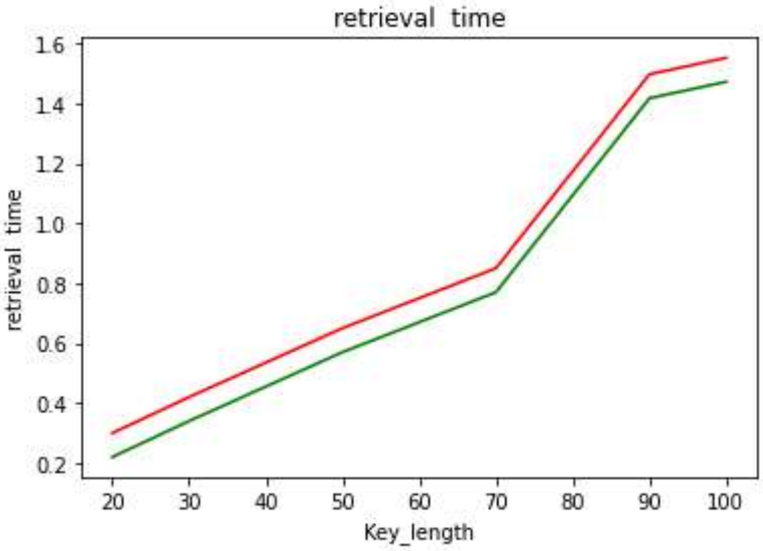


Figure 7: Graph of retrieval time

Implementing the method increases the retrieval time from the starting place to the final location, as depicted in the figure 7. During this time there is a significant likelihood of security when uploading personal information. At the final stage the accuracy is 98%.

Loss vs Epoch

Loss: The value of the loss metric calculated across the training data at the end of each epoch is referred to as "loss." Because of this, the optimization process is working to reduce it as much as possible through the training; hence, the lower it gets, the better. Additionally, to determine the loss for each epoch, add the result to the column for train losses for each epoch after deducting the running loss from the total number of batches.

Epoch: One pass through the entire dataset used for training is referred to as an epoch. A neural network must often be trained over a number of iterations, or epochs. During the process of training the model, one of the scalar values that we work to reduce is called loss.

Table 3 - Comparison of Loss

EPOCH	RSA	Blowfish	MD5	Proposed
20	0.49	0.52	1.43	0.40
40	1.40	0.43	1.55	0.30
60	0.33	0.35	0.21	0.15
80	0.28	0.51	0.25	0.10
100	0.19	0.32	0.11	0.05

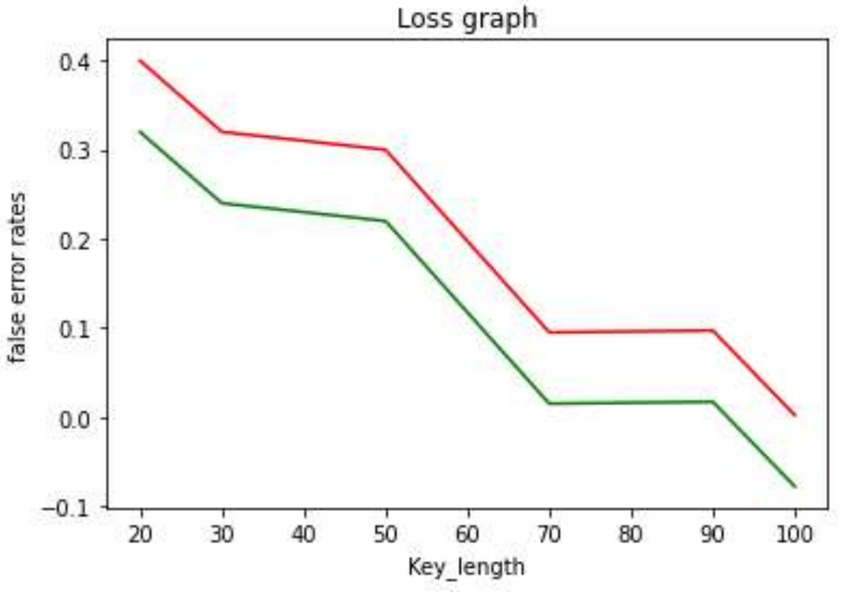


Figure 8: Representation of Loss Epoch Security in Cloud

Implementing the method decreases the loss from the starting place to the final location, as depicted in the figure 8. During this time there is a significant likelihood of security when uploading personal information and there is almost negligible loss percentage.

Throughput time vs Epoch

Throughput Time: The amount of time required to encrypt plain text into cypher text is the unit of measurement used to determine the length of the encryption process. The following is an expression of the mathematical formula for calculating the encryption time:

ET= Endtime – Starttime (for encryption process)

It is a representation of the encryption time based on the equation above. Milliseconds are used to measure the length of time required for encryption (ms). Hence proposed hybrid technique reduces the throughput time.

Table 4: Comparison of Throughput Time

EPOCH	RSA	Blowfis h	MD5	Proposed
20	0.54	0.42	1.56	0.41
40	1.45	0.41	1.35	0.34
60	0.23	0.25	0.32	0.18
80	0.31	0.54	0.36	0.11
100	0.16	0.36	0.19	0.09

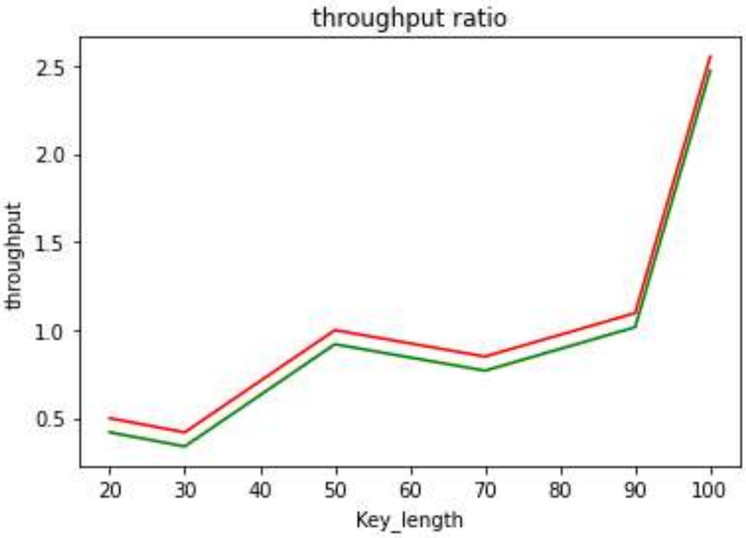


Figure 9: Throughput Time during Cloud Computing

Storage time vs Epoch

Storage Time: The length of time required to transform the encrypted text into plain text is what is meant when people talk about the decryption time. The mathematical formula for the amount of time required to decrypt a message can be written out as presented below.

ST= Endtime - Starttime (for storage process)

It is the time required to decrypt the message based on the equation presented above. The amount of time required to decrypt a message is expressed in milliseconds (ms). The longer the length of the decryption time, the less likely it is that the technique will work as expected.

Table 5: Comparison of Storage time

EPOCH	RSA	Blowfis h	MD5	Proposed
20	0.53	0.46	0.43	0.40
40	1.11	0.43	1.15	0.33
60	0.35	0.23	0.42	0.19
80	0.36	0.34	0.15	0.09
100	0.19	0.26	0.16	0.08

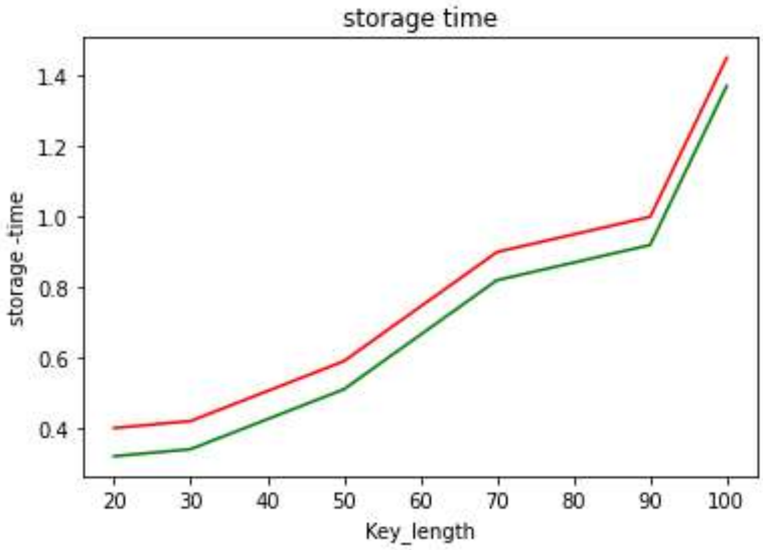


Figure 10: Storage Time during Cloud Computing

The above observations can be made by using eclipse to run varying input size both locally and on Google App engine. This observation can be made using the tabular results and the graph results. Below all algorithm MD5, a symmetric encryption algorithm, is the one that takes the least amount of time, and above all algorithm fish, the one that takes the most. MD5 is a symmetric encryption technique, and the speed-up ratio drops dramatically as the input size grows. The speed increase ratio for the MD5 algorithm is the highest, followed by RSA. The RSA requires a smaller buffer size and a shorter amount of time to encrypt and decrypt data when compared to MD5 and RSA. On the other hand, RSA requires a larger buffer size and a longer amount of time when compared to MD5 and Blowfish. Therefore, the above result is a draw if we compare various algorithms in terms of buffer size; however, the MD5 algorithm is the one that we favour.

TOOLS USED

Spyder (Python 3.9), Google Firebase Cloud, and Anaconda Navigator were utilized to develop the entire framework.

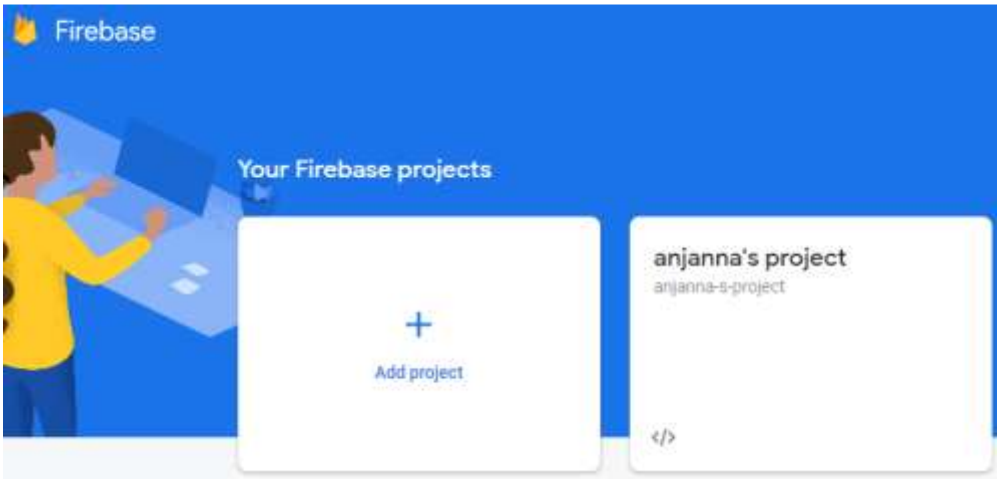


Figure 11: Home page of Google Firebase Cloud

Figure 11 depicts the homepage of cypher cloud; to begin, the user must click Login/Signup.

As Cipher cloud relies on Google Accounts for authentication, the Sign in page will direct the user to sign in with his or her Google Account ID and password. Since the user is new in this case, Cipher Cloud requests authorization to create a new account using the Google Account that the user was logged in with. On this page, the user has the option to select the algorithm he or she wishes to utilize for this particular account. Once selected, the algorithm cannot be altered.

CONCLUSION

Although cloud computing has a lot of benefits, there are still a lot of real issues with it that need to be fixed, especially when it comes to security. If we are successful in eradicating or mastering this security vulnerability, the future will consist of solutions for cloud storage used by both large and small businesses. Implementation of our algorithm ensures the confidentiality of the data. The data is inaccessible to everyone but the authorised user. Even in the event that an intruder (an unauthorised user) unintentionally or purposely obtains the data and is unable to decode it since it requires two keys originating from two distinct locations.

Each person uses cloud computing differently, although many find it useful. The cloud's flexibility is attracting data migration. The cloud lets organizations store a lot of data and access it whenever they need it. When more people store sensitive data on the cloud, it becomes difficult to store safely. RSA, MD5 and Blowfish are data security algorithms. In contrast to RSA, these symmetric key techniques employ the same key for both encryption and decryption. These algorithms must be made secure. Cloud computing manages security risks well. This study found that RSA, MD5 and Blowfish are the best encryption algorithms for performance. If data security is an issue, use MD5. MD5 buffer size is also good.

REFERENCES

1. Kumar, G. S., Premalatha, K., Aravindhraj, N., Nivaashini, M., & Karthiga, M. (2019). Secured cryptosystem using blowfish and RSA algorithm for the data in public cloud. International Journal of Recent Technology and Engineering (IJRTE) ISSN, 2277-3878.
2. Gitanjali, K. L. (2019). A novel approach of sensitive data classification using convolution neural network and logistic regression. Int J Innov Technol Explor Eng, 8(8), 2883-6.
3. Li, Y., Gai, K., Qiu, L., Qiu, M., & Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences, 387, 103-115.
4. Kanchanadevi, P., Raja, L., Selvapandian, D., & Dhanapal, R. (2020, October). An Attribute Based Encryption Scheme with Dynamic Attributes Supporting in the Hybrid Cloud. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 271-273). IEEE.
5. Rani, P. K., Sathiya, S., Sureshkumar, S., & Kumar, B. A. (2022, May). Enhancing Cloud Security with Hybrid Encryption. In 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1445-1450). IEEE.
6. Murad, S. H., & Rahouma, K. H. (2022). Hybrid Cryptography for Cloud Security: Methodologies and Designs. In Digital Transformation Technology: Proceedings of ITAF 2020 (pp. 129-140). Springer Singapore.
7. Abroshan, H. (2021). A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. International Journal of Advanced Computer Science and Applications, 12(6), 31-37.
8. Orobosade, A., Aderonke, T., Boniface, A., & Gabriel, A. J. (2020). Cloud application security using hybrid encryption. Communications, 7, 25-31.

9. Taha, A. A., Abdelminaam, E. D. D. S., Khalid, M., & Hosny, K. (2017). Enhancement the security of cloud computing using hybrid cryptography algorithms. Int. J. Adv. Comput. Technol, 9(3), 36-42.
10. Hagge M, von Hoffen M, Betzing J, Becker J (2017) Design and implementation of a toolkit for the aspect-based sentiment analysis of tweets, pp 379–387
11. Zhou X, Tang X (2011) Research and implementation of RSA algorithm for encryption and decryption. In: Proceedings of 2011 6th international forum on strategic technology, vol 2. IEEE, pp 1118–1121
12. Chauhan A, Gupta J (2017) A novel technique of cloud security based on hybrid encryption by blowfish and md5. In: 2017 4th International conference on signal processing, computing and control (ISPCC). IEEE, pp 349–355
13. Sachdev A, Bhansali M (2013) Enhancing cloud computing security using AES algorithm. Int J Comput Appl 67(9)
14. Nicholas, K., Wilson, C. H. E. R. U. I. Y. O. T., & Kibe, A. (2017). Enhancing trust in cloud computing using MD5 hashing algorithm and RSA encryption standard. International Journal of Scientific and Engineering Research, 8(3), 550-566.
15. Bangar A, Shinde S (2014) Study and comparison of cryptographic methods for cloud security. Int J Comput Sci Eng Inf Technol Res 4(2):205–213
16. Gunasekaran S, Lavanya MP (2015) A review on enhancing data security in cloud computing using RSA and AES algorithms. Int J Adv Eng Res 9(4):1–7
17. Kartit Z, Azougaghe A, Idrissi HK, El Marraki M, Hedabou M, Belkasmi M, Kartit A (2015) Applying encryption algorithm for data security in cloud storage. In: Sabir E, Medromi H, Sadik M (eds) Advances in ubiquitous networking. Springer, Singapore, pp 141–154
18. Yugandhara K, Ashwini J, Pooja P, Suchita P, Pawar JS (2016) Secure data storage and forwarding in cloud using AES and HMAC. Int Res J Eng Technol 03(02):75–79
19. Salem MZ, Sabbeh SF, EL-Shishtawy T (2017) An efficient privacy preserving public auditing mechanism for secure cloud storage. Int J Appl Eng Res 12(6):1093–1101
20. Cordova, R. S., Maata, R. L. R., Halibas, A. S., & Al-Azawi, R. (2017, November). Comparative analysis on the performance of selected security algorithms in cloud computing. In 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA) (pp. 1-4). IEEE.
21. Jain, G., & Sejwar, V. (2017, June). Improving the security by using various cryptographic techniques in cloud computing. In 2017 International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 23-28). IEEE.
22. Singh, S. K., Manjhi, P. K., & Tiwari, R. K. (2016). Data security using RSA algorithm in cloud computing. International Journal of Advanced Research in Computer and Communication Engineering, 5(8), 11-16.
23. Pannala, N. U., Nawarathna, C. P., Jayakody, J. T. K., Rupasinghe, L., & Krishnadeva, K. (2016, December). Supervised learning-based approach to aspect based sentiment analysis. In 2016 IEEE international conference on computer and information technology (CIT) (pp. 662-666). IEEE.
24. Cao, D., Ji, R., Lin, D., & Li, S. (2016). Visual sentiment topic model based microblog image sentiment analysis. Multimedia Tools and Applications, 75, 8955-8968.