International Journal of Research in Engineering, Science and Management
Volume 4, Issue 5, May 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

Analysis of Security Algorithms in Cloud Environment

Simranjeet Kaur[1*], Prajakta Shinde[2], Jueily Joshi[3], B. S. Dakhare[4]
[1,2,3,4]*Department of Information Technology, Bharati Vidyapeeth College of Engineering, Navi Mumbai, India*

***Abstract*: Cloud computing is a virtual pool of resources and it provides these resources to users via the internet. People are storing their huge amount of data over the cloud. In recent years, Storage in Cloud gained popularity among both companies and private users. However, data privacy, security, reliability and interoperability issues still have to be adequately solved. But the most important problem is security and how cloud provider assures it. For ensuring privacy there are multiple encryption algorithms. Encryption is the process of encoding information or data precisely to prevent unauthorized access. This paper discusses the comparison of various cryptographic encryption algorithms with their various key features & then later discusses their performance cost based on the encryption time, decryption time, power consumption, memory usage, latency and security level. Moreover, this paper has compared the efficiency of each algorithm in cloud computing. The comparison will be between symmetric key algorithms which will include blowfish, AES-256 algorithm, Asymmetric algorithms like RSA, hybrid algorithms like RSA with AES-256 and RSA with blowfish.**

***Keywords*: Symmetric key Algorithms, Asymmetric Key Algorithms, hybrid, Encryption & Decryption time, Data security.**

1. Introduction

Cloud computing is described in different computing concepts which contains a huge number of computers attached through real-time communication like INTERNET. Cloud computing provides IT services as on-demand services, accessible from anywhere, anytime by anyone. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. It provides the shared pool of resources, including data storage space, networks and specialized corporate and user applications. This is based on an encryption/decryption algorithm that aims to protect the data stored in cloud from the unauthorized access.

Encryption is the way of converting a plaintext message into ciphertext that can be decoded back into the original message. Asymmetric cryptography is a class of cryptographic algorithms that requires two separate keys, one of which is public. Public key is used to encrypt plaintext; whereas private key is used to decrypt ciphertext or to create the digital signature. Symmetric-key algorithms are a class of algorithms for cryptography that uses the same cryptographic key for both encryptions of plaintext and decryption of ciphertext. The key represents the shared secret between two or more parties that can be used to maintain information links.

Security in cloud computing involves concepts such as network security, equipment and control strategies deployed to protect the data, applications and infrastructure associated with cloud computing. Security measures will be adopted to prevent unauthorized access, copying, using or modifying personal information. The data also should be encrypted when transmitted across networks to protect against eavesdropping of network traffic by third-party users. It describes our model proposed of securing data in cloud storage algorithm for encryption/decryption for outsourcing data in cloud storage.

In our paper, we also represent the hybrid cryptography algorithms that efficiently encrypt the transmitted data through the cloud for better security and best results. Users will have different varieties to encrypt or decrypt their own data with any of hybrid algorithms based on the time consumed by the algorithm to encrypt the data. In our paper, we also provide the complete encryption scheme, selection of algorithms for encryption and decryption.

2. Literature Review

[1] A Comparative Analysis of security algorithms using cryptographic techniques in cloud computing by R. Gowthami Savanya, and A. Kausalya gives us a theoretical comparison of symmetric and Asymmetric cryptography algorithms.

[2] Developing new hybrid cryptography algorithms for cloud computing by Ali abdulridha Taha, Dr. Diaa Salama Abd Elminaam, Prof. Dr. Khalid M. Hosny describes hybrid cryptography algorithm allows the user to encrypt his data with hybrid encryption algorithms with two strong encryption algorithms without taking large time in encrypting data.

[3] Data Security in cloud computing using AES under HEROKU cloud by Bih-Hawang Lee, Ervin Kusuma Dewi, Muhammad farid wajdi discusses data security in cloud computing using AES under Heroku cloud. They implement Heroku cloud as cloud computing platform, then they implement AES in the website to secure data.

[4] A Multi-Threaded Symmetric Block Encryption Scheme Implementing PRNG for DES and AES Systems by Adi A. Maaita, Hamza A. Alsewadi forms an application of proposed PRNG algorithm modification as part of the sub-key generation process within AES and DES algorithms have resulted in

*Corresponding author: johalsimran555@gmail.com

considerable improvements in the diffusion attribute of both algorithms.

[5] An analysis of Its Challenges & Cloud Computing by M. D. K. Kumar, G. V. Rao, and G. S. Rao they compare existing symmetric algorithms like DES, Blowfish, 3DES, AES, RSA, DSA, Diffie Hellman Algorithm, ELGAMAL on the basis of different parameters which includes Block size, key length, security and speed.

3. Algorithms Used

A. AES

Advanced Encryption Standard (AES) is a symmetric key block cipher. The cipher has a variable block length and key length. It encrypts information in single block cipher and does so one block at a time that is known as rounds. During encryption and decryption process, AES system goes through same rounds depending upon their key length that is 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for the 256-bit keys in order to deliver the final cipher-text

B. Blowfish

Blowfish is another symmetric encryption and it designed as a block cipher like AES but the key length goes from 32bits to 448 bits. It splits messages into blocks of 64bits and encrypts them individually. This encryption algorithm was specially designed to encrypt the data on 32-bit microprocessors. The difference with the other encryption algorithms is that it utilizes about 16 rounds of encryption which is depend on the key or data size.

C. RSA

Rivest-Shamir-Adleman (RSA) is an asymmetric cryptographic algorithm and it is known for public key cryptosystem for exchange or digital signature or encryption block of data. Sender encrypts message using the receiver public key and when message gets transmit to receiver, then receiver can decrypt it by using it's own private key. Key size is 1024 to 4096 bits. It is also based on factoring problem of finding product of two large prime numbers. RSA is more intensive than AES, and much slower. It's used to encrypt only small amount of data.

D. Hybrid Algorithm

Indeed for better performance and high feasibility we have used hybrid algorithms. We have researched and found that hybrid algorithm have huge scalability compared to other algorithms. Therefore, we have implemented two hybrid algorithms.

RSA with AES and RSA with blowfish are the two different hybrid algorithms which we have implemented especially for the data security in cloud.

4. Implementation

This paper discusses and compares different existing encryption algorithms especially in the context of data security in the cloud. Users will have different varieties to encrypt and decrypt their own data with any of the algorithms based on the time consumed by the algorithm to encrypt the data and the level of security provided by this algorithm. Also, the proposed work shows the points of strengths and weaknesses of encryption algorithms. This suggests the encryption of the files should be uploaded on the cloud. The integrity and confidentiality of the data uploaded by the user are ensured doubly by not only encrypting it but also providing access to the data only on successful authentication. The existed file on the device will be encrypted using different algorithms. To enhance security; The authorized user can also download any of the uploaded encrypted files and read them on the system.

Parameters mentioned below are the metrics we have implemented:

A. File Upload

This algorithm got two phases. In the first phase, the algorithm encrypts Ciphertext with the user's selected Algorithm. In the second phase, we encrypt the key using the selected algorithm. It permits sending an encrypted file in Cloud storage.

B. File Download

This algorithm also includes two phases, in the first phase, the algorithm decrypts the key using the selected Algorithm. In the second phase, it decrypts ciphertext using a key retrieved from the server.

C. Implement results and analysis

This is the section where analysis of different algorithms will be shown in graphs as results.

It includes:

1. Execution time for encryption for different algorithms.
2. Execution time for decryption for different algorithms.
3. Execution time by file size for different algorithms.

The implementation platform for the system will be a python framework called Django Framework with other components like cryptography library. We have used PythonAnywhere.com for hosting our website on cloud. We have used cloud basically for storage. The database for the system will be SQLite.

1. Python (version- 3.7.4)
2. Cryptography
3. Django Framework.
4. SQlite

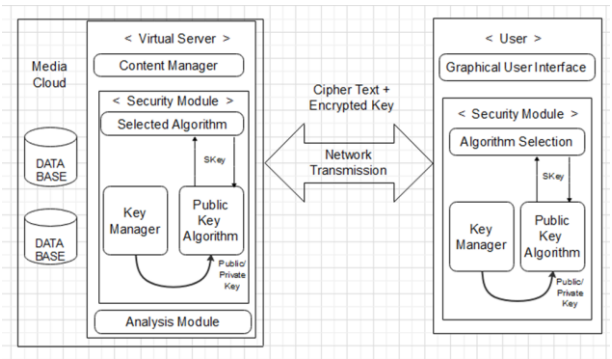

Fig. 1. System structure

The proposed hybrid cryptography algorithm developed to

secure the data and information which is transmitted through the cloud. The aim of the hybrid cryptography algorithm is to efficiently encrypt and secure the transmitted data. Four algorithms were implemented in the project. Two of these algorithms are hybrid and implemented to improve the efficiency of the encryption algorithm time and security. Using the hybrid algorithms improves the security of the files uploaded since that the data is encrypted using more than one algorithm and at the same time minimize the time taken by the algorithms that takes much time to encrypt the data. Figure 1 shows the basic system structure from scratch to end.

5. Evaluation Parameters

Each of the encryption techniques has its own strong and weak points. To order to apply a suitable cryptography algorithm to an application, we should know the performance, strength and weakness of the algorithms. Therefore, these algorithms must be analyzed based on several features. In our paper, analysis is done with the following metrics under which the cryptosystems can be compared are described below:

A. Encryption time

The time taken to convert plaintext to ciphertext is encryption time. Encryption time depends upon the key size, plaintext block size and mode. In our experiment, we have measured encryption time in milliseconds. Encryption time impacts the performance of the system. Encryption time must be less making the system fast and responsive.

B. Decryption time

The time to recover plaintext from ciphertext is called decryption time. The decryption time is desired to be less similar to encryption time to make the system responsive and fast. Decryption time impacts the performance of the system. In our experiment, we have measured decryption time in seconds.

C. File size

The size of the file in MB. We have made sure that it can be any type of file for eg. Images, Audio, Video, Text and CSV files as well.

6. Results

In this section, we discuss the results obtained based on three evaluation parameters.

A. Client Side

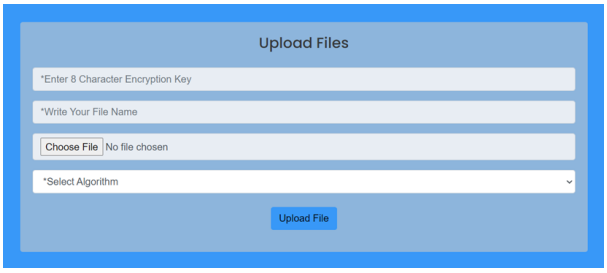

Fig. 2. Upload section

This is the upload section for uploading files for the clients where they have to enter a password (encryption key) with the file name and the user also has the liberty to choose the algorithm which suits their requirements best based on the data and the file size they choose to upload.

B. Encryption time, Decryption time

Fig. 3. Encryption and Decryption time w.r.t file size

In figure 3, We have created different buckets in which the files have been uploaded respectively according to the requirements. It includes all types of files like Images, Videos, Text and Excel Sheets\CSV. We have used all the algorithms in order understand emphasize the motto of our project. It also shows the file size and date uploaded for more effective understanding and for maintaining good CRM. The encryption time and decryption time are mentioned as well and we can see the difference precisely. Time in sec helps to ensure and maintain the effectiveness and the best results from the respective algorithms.

The aim of the proposed hybrid cryptography algorithm is to determine the fastest and secure encryption algorithm of the previous presented encryption algorithms. It also allows the user to choose the encryption algorithm which is more suitable for the type of his own data. The proposed hybrid cryptography algorithm offers set of encryption algorithms:

1) Hybrid algorithm using RSA and AES algorithm.
2) Hybrid algorithm using RSA and Blowish algorithm.

In Hybrid algorithm, several steps have to be done to encrypt and decrypt the file. To encrypt the file the algorithm will work as follow:

1. RSA has two keys that is public and private key, where public key is used in encryption and private key is used in decryption.
2. After uploading a file, RSA's public key and the user generated key while uploading are being encrypted which is known as encrypted key, and this encrypted key is added to the file.
3. The encrypted file is again being encrypted with AES key.
4. In order to decrypt, decryption

AES key is used to get the same original decrypted file.

C. Graph (Chart Analysis)

In this figure we can see that the on X-axis we have the file size which we have uploaded that is 1.2424MB and we have got the encrypting time(sec) of AES-256, Blowfish and two hybrid algorithm that is RSA & Blow fish and RSA & AES respectively.

We can determine that RSA&AES which is a hybrid algorithm is the best since it only takes 3.768 seconds which is the least time as compared to all other algorithms.

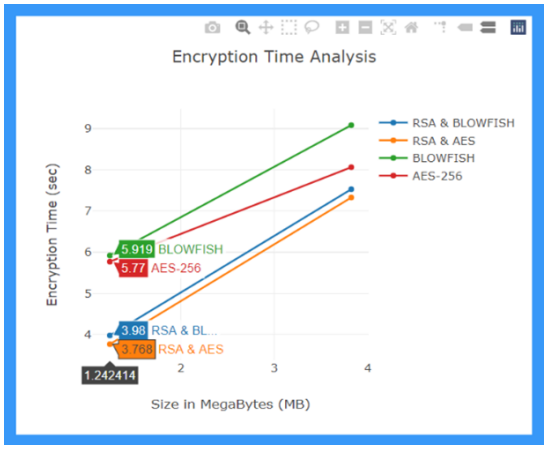

Fig. 4. Chart Analysis (Encryption)

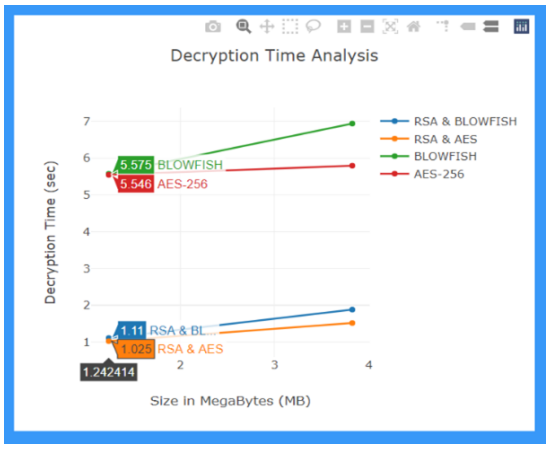

Fig. 5. Chart Analysis (Decryption)

This is the figure where decryption is being done for the securing the original uploaded file at client side.

We can see that the hybrid algorithm which is RSA & AES requires least time even for decryption, thus resulting in one of the best algorithms.

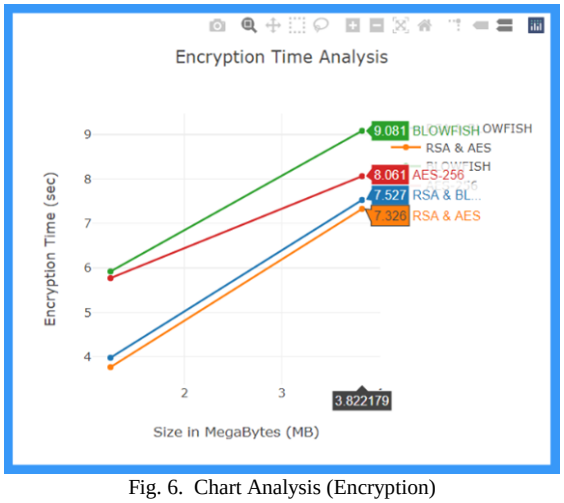

Fig. 6. Chart Analysis (Encryption)

In this figure for more accurate results we have uploaded one more file with the size of 3.822179 for all the respective algorithms.

We have attained that hybrid algorithm that is mixture of two algorithm that is RSA & AES requires the least time as compared to all other algorithms irrespective to the file size.

On the other hand we presumed that Blowfish algorithm takes the highest time for encrypting the file unloaded.

Thus we can explicitly mention that even if the file size is more the hybrid algorithm will be best.

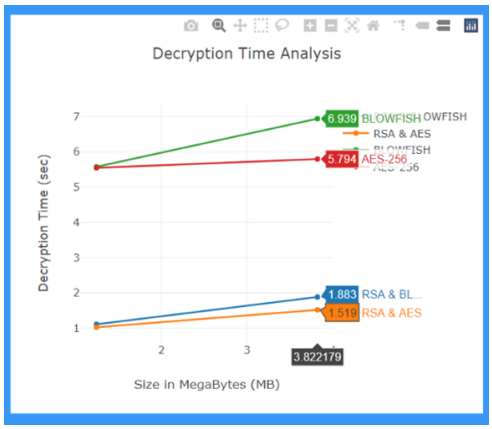

Fig. 7. Chart Analysis (Decryption)

Here decryption is being done for securing the original uploaded file at client side.

We can see that the hybrid algorithm which is RSA & AES requires 1.591 sec for the file size of 3.822 which is the least time.

On the other hand, even for decryption we have assumed and implemented that Blowfish algorithm needs more time among all of the other algorithm whereas the hybrid algorithm RSA & Blowfish also performs better together with 1.88 sec for the given file which differ slightly. Thus as a result hybrid algorithms are the finest and foremost algorithm.

D. Final Results

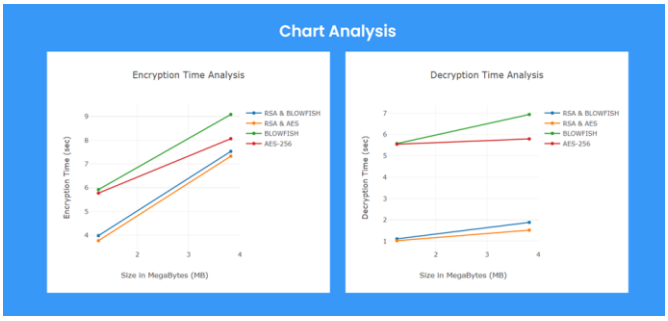

Fig. 8. Chart Analysis (graph)

These are the final results\analysis we have shown in the form of charts. On the left side, we have the encryption time and on the right side, we have decryption time which allows us to visualize the results to all the algorithms. We can see that Blowfish takes the highest time for encryption and decryption, and RSA with AES takes the least time for encryption and decryption, being fastest. Blowfish consumes the most time

among all. Thus we have concluded that hybrid algorithm is efficient and can be used in future work.

7. Conclusion

Data security has become the most important issue in cloud computing security. The data or information should not be leaked to the third¬-party user efficient security algorithms should be implemented. We compare the encryption and decryption times that encrypted and decrypted different sizes of files. Hybrid cryptography algorithms represent the variety of encrypting algorithm that allows user to choose the algorithm for encryption which is suitable with his own type of data. The hybrid cryptography algorithm improves the performance of the encryption algorithms since it encrypts the data in a minimum time and insecure way. Results show that. The cloud computing framework presented in our project can be extended by adding new hybrid algorithms constructed from different existing algorithms to improve the encryption process and compare it with the results of current work. The proposed system proves that using hybrid algorithms increases the level of securing the encrypted transmitted data and also minimizes the time taken to encrypt it.

References

[1] R. Gowthami Savanya, and A. Kausalya, A Comparative Analysis of security algorithms using cryptographic techniques in cloud computing," International Journal of Computer Science and Information Technologies, Vol. 8 (2), 2017, 306-310.

[2] Ali abdulridha Taha, Dr. Diaa Salama Abd Elminaam, Khalid M. Hosny, "Developing new hybrid cryptography algorithms for cloud computing by compares symmetric and asymmetric cryptography algorithm." IJACSA, vol. 8, no. 8, 2017.

[3] Adi A. Maaita, Hamza A. Alsewadi M. Shabbir and Y. Al-Nabhani, "A Multi-Threaded Symmetric Block Encryption Scheme Implementing PRNG for DES and AES Systems," IJACSA, vol. 8, no. 2, 2017.

[4] Ritu Tripathi, Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques," International Journal of Innovative Research in Advanced Engineering, March 2016.

[5] Mashrufee Alam et. al., A Comparative Study of RSA and ECC and Implementation of ECC on Embedded Systems algorithms, March 2016.

[6] Ritu Pahal, Vikas Kumar, "Efficient Implementation of AES," in IJARCSSE, vol. 3, no. 7, July 2013.

[7] W. Y. Zibideh and M. M. Matalgah, Phoenix, "Modified DES Encryption Algorithm with Improved BER Performance in Wireless Communication," pp. 219-222, Jan. 2011.

[8] E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16-Round DES," Proceedings of Crypto, vol. 740, Santa Barbara, CA, December 1991.

[9] Modes of Operation Validation System for the Triple Data Encryption Algorithm, NIST Special Publication 800-20, National Institute of Standard and Technology, 2000.