iJRASET
International Journal For Research in
Applied Science and Engineering Technology

Volume: 10 Issue: V Month of publication: May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42652

File Storage on Cloud Using Cryptography

Utkarsha Kulkarni[1], Rosemeen Mansuri[2], Riya Adikane[3]
[1, 2, 3]*Department of Electronics and Communication Usha Mittal Institute of Technology*

Abstract: Hybrid cryptography is implemented to provide the multilevel of encryption and decryption at both sender and receiver side which increase the security of the cloud storage. This security model gives the transparency to the cloud user. The hybrid encryption algorithm combines the advantages of fast encryption speed of AES algorithm, easy management of RSA algorithm key, and digital signature to ensure the secure transmission of confidential documents. Data/information is the most valuable asset for the modern electronic communication system. Securing data or information has become a challenge in this competitive world. There are many techniques for securing data/information such as cryptography, stenography etc. In this paper, hybrid cryptography has been applied using AES and RSA.AES and RSA algorithms are implemented to provide the multilevel of encryption and decryption at both sender and receiver side which increase the security of the cloud storage. This approach provides transparency to the cloud user as wellas cloud service provider in order to reduce the security threats. The proposed model is implemented in C and .NET. Data security is increased up to a maximum extent and it takes less time in uploading and downloading the text file as compare to existing system. [1]

Index Terms: Hybrid, Symmetric, Asymmetric, Cloud, Cryptog-raphy.

I. INTRODUCTION

Cryptography technique translates original data into unread- able form. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only authorized person can access data from cloud server. Cipher text data is visible for all people. Cryptography is used by security professionals for various reasons but the three main reasons for using cryptography are: Data Confidentiality, Data Integrity and Data Authentication [3]. Confidentiality or data privacy is the most important goal of cryptography hence the meaning of a message is encoded to conceal it. The sender usesa cryptographic key to encrypt the message and the recipient also uses the same or a different cryptographic key to decrypt or decode the message. Data integrity involves ensuring that the message received is similar to the sent message i.e it has not been modified or altered in any way. A unique message digest is created using hashing from the sent message and using the same technique, the recipient creates a second digest from the received message for comparison with the original one [3]. The most simplest form of encryption is known as the Caesar’s cipher which is done by simply shifting each lettera set of spaces up or down the alphabet. There are primarily4 main types of cryptography in use today each with its own set of advantages and disadvantages [3]. delivery hence it is not suitable for communications over internet [2].

1) *Asymmetric Cryptography:* As the name suggests it has two different keys for encryption and decryption. The first keyis a public key which is used for encryption at sender side and the second is private key which is used for decryption at receiver side [2].
2) *Key Exchange Algorithms:* Although not being used for encryption but it has a significant purpose as it provides a way to securely exchange keys which are generated by the symmetric or asymmetric algorithms [2].
3) *Hybrid Cryptography:* As the name suggests it is made up of two algorithms which are blended with each other in order to provide increase security. PGP is a well known hybridalgorithm used in security of e-mail communications. [2] The following two algorithms will be used for developing the hybrid algorithm:

a) *RSA algorithm* - accounts for the primary encryption of the file.
b) *AES algorithm* -generates a secret key to decrypt and download the file.

II. LITERATURE SURVEY

In The paper we avoids use of LUTs and proposes use of composite field data path for the SubBytes and InvSubBytes transformations. The use of such data paths is the key for the de- sign of high-speed subpipelined AES architectures [4]. A hybrid encryption algorithm mixing AES and RSA algorithms is suggested in this paper to overcome the above issues in orderto solve file encryption performance and security problems. The experimental results suggest that the RSA and AES hybrid encryption algorithm can not only encrypt files, but also pro- vide the benefits of efficiency and protection of the algorithm

[5]. Khairnar, Dr. Vaishali Kadam, K. (2015). Hybrid RSA- AES Encryption for Web Service presents a method which enhances security for data by hybrid encryption, which can be used itself as end-to-end encryption or in addition to the existing SSL. This enhances security of data exchange between two clients using web service as an intermediary. The proposed solution encrypts the content block which canbe only decrypted by client side, and not on the web server [6]. In the paper is proposed two new hybrid algorithms using combination of both symmetric and asymmetric cryptographicalgorithm such as Twofish, AES, RSA and ElGamal. To analyze results was used JAVA program implementation. The results shows that the proposed hybrid algorithm AES+RSA issignificantly secure. However, Twofish + RSA hybrid has otheradvantages like better computation time, the size of cipher text, and the memory consumption [7].To overcome the tech- nique problem of key management and database encryption in the implementation process of database encryption system, some difficult technology of encrypt/decrypt engine in the implementation process are discussed, the hybrid cryptographyencryption program is presented based on IDEA combined with RSA, and the encryption system is designed and realized [8].In this paper a hybrid cryptography algorithm is proposed in order to achieve confidentiality and increase security in the communications taking place over the internet. The paper also focuses on the time taken for the encryption and decryption process so that the algorithm is not CPU exhaustive [9].This paper concluded that the proposed method provides high secu-rity on data transmission over the internet and proper network access on demand to a shared tank of constructive computing resources, mainly net, server, and storage application [10].

III. RSA ALGORITHM IN CRYPTOGRAPHY

RSA algorithm is an asymmetric cryptographic, because it use different keys for encryption and decryption. It consists of three major steps in encryption and decryption .

1) *Key Generation:* In this step two keys are generated. Public key: it used in public for encrypting. Private key: this key is accessed by the receiver only for decrypting. The process for key generation works as fol- lows: First choose two distinct prime numbers p and q and then compute n=pxq where n isthe modulus for the public key and the private keys.

(n) = (p 1)(q 1) (1)

Next compute Choose an integer e such that1 ¡ e ¡ (n) and GCD (e, (n)) = 1 (2)

The pair (n, e) is the public key.

The private key is a unique integer d obtained by solving theequation e 1(mod(n)) (3)

2) *Encryption Method:* Is used for encrypting an image or textby using public key.

The messege (m) is presented as pixels in the range from 0 to255.

The text is encrypted using the public key (n, e) from theequation

c = me mod (n) (4)

3) *Decryption Method:* The text or image is decrypted using theprivate key (n,d). m = c d mod (n), [11].

IV. AES ALGORITHM IN CRYPTOGRAPHY

AES algorithm belongs to a block cipher of symmetric cryptography. The rounds of repeated transformations in this algorithm are called round transformation. There are 3 typesof round transformations called initial round, repeating round and final round. Each round includes processes of SubBytes, ShiftRows, MixColumns and AddRoundKey, and the final round does not have a MixColumns process. The process of SubBytes is to replace the data of 4×4 state matrix intothe corresponding data in SubBytes table according to the algorithm [12]. The process of ShiftRows is to implement left cyclic shift on the data in state matrix. It means that the first row of the matrix remains unchanged, the second row is left-shifted by1 byte, the third row is left-shifted by 2 bytes, and the fourth row is left-shifted by 3 bytes. The process of MixColumns is pre-multiplying MixCol- umns matrix with state matrix. The process of AddRoundKey is to perform a bitwise XOR operation on data and round key. The process of ExpandKey is to generate round keys by using Recursive Algorithm, usinginitial key as the initial state of a recursive equation and generating a group of round keys per round [12].

V. PROPOSED SYSTEM

Hybrid Cryptography RSA is a public key encryption tech- nique based on hybrid theory .It is used to create faster, smaller, and more efficient cryptographic keys. RSA keys are generated through the properties of the hybrid equation insteadof the traditional method of generation as the product of very large prime numbers.RSA is becoming widely used for mobileapplications because it helps to establish equivalent security with lower computing power and battery resource usage. RSAwas developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturerof integrated circuitry (IC) and network security products.

An hybrid is represented as a looping line intersecting two axes (lines on a graph used to indicate the position of a point) and not an ellipse (oval shape).
RSA is based on properties of a particular type of equation created from the mathematical group (a set of values for whichoperations can be performed on any two members of the groupto produce a third member) derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result. The derived equations have a characteristic that is very valuable for cryptography purposes they are extremely difficult to reverse and relatively easy to perform. Both clouds agree to some publicly-known data item.
The hybrid equation

1) Values of a and b
2) Prime, p

The elliptic group computed from the hybrid equation lower security can also be employed. It is also possible to combine another algorithm that will encrypt data given by the IDEA algorithm. This inclusion of third algorithm will increase the security but there are two sides to a coin. As a result Security will increase but time that is taken to convert the plain text into final cipher text will be greater than previoushybrid algorithm. So it is the demand of application in which the user is going to use security algorithm ,which factor is important time or security. A fair role must be played betweentime taken by the algorithm and level of security, both must be reasonable [13].

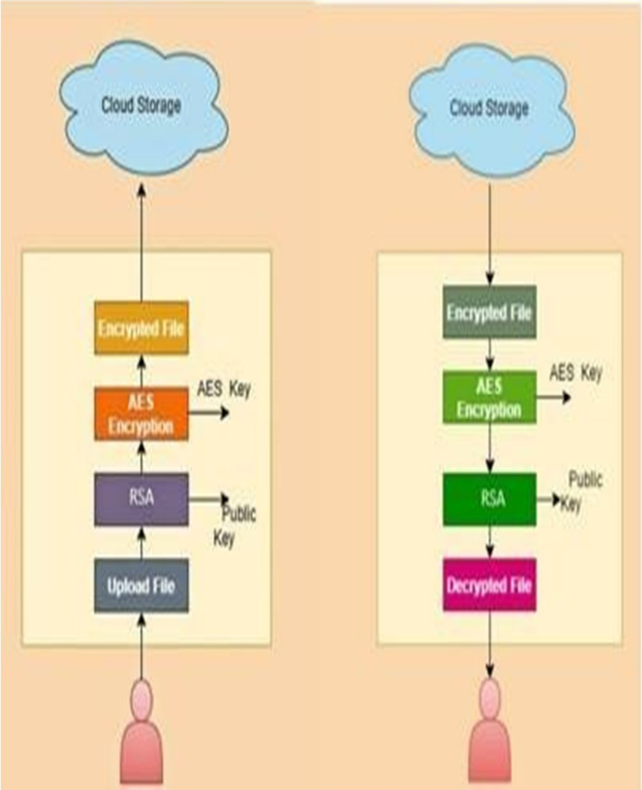


Fig. 1. Encryption And Decryption Process on the Web Page

VI. CONCLUSION

After studying the cryptographic model, the conclusion is that data security is the most considerable topic related to cloud computing technology. The integration between sym- metric and asymmetric cryptosystems is employed to over- come security limitations .User would try to secure sensitive data on the cloud by applying the hybrid of different en- cryption algorithms such as RSA and AES. This study also concludes that hybrid cryptography enhances the performance and adds more security levels to the data compared to applying these algorithms individually. All of the examined studies have benefits and some drawbacks. In the future, we aim to overcome these drawbacks to enhance security, integrity and performance.

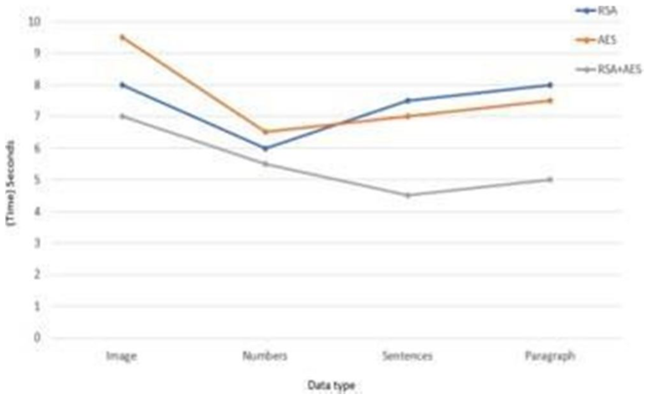


Fig. 2. Time Graph

A base point, B, taken from the elliptic group Encryption and Decryption Process is shown in figure 1 and figure 2 showsthe Time graph of all the algorithms with different types of data.

VII. RESULT

Hybrid cryptography using RSA and AES algorithm enablesuser to secure data safely on cloud and makes it accessible only to people who have the secret key .Even a minor error in the secret key would lead to error in encryption and decryption.The web application (.NET) is connected to user’s Gmail account and sends the Username,password and secret key via mail.Data can be uploaded in text and image format. This data is stored on cloud in encrypted format and can be decrypted and downloaded using secret key.

VIII. FUTURE SCOPE OF HYBRID CRYPTOGRAPHY

The proposed hybrid algorithm can be made much more powerful and secure by increasing the number of iterations in the encryption algorithm to suit the level of security required. An inverse policy of reducing the number of iterations for

REFERENCES

[1] S. Kumar, G. Karnani, M. S. Gaur and A. Mishra, ”Cloud Security using Hybrid Cryptography Algorithms,” 2021 2nd International Conference onIntelligent Engineering and Management (ICIEM), 2021, pp. 599-604, doi: 10.1109/ICIEM51511.2021.9445377.

[2] L. Ji-Zhong, J. Lie-Hui, Y. Qing and X. Yao-Bin, ”Hybrid Method to Analyze Cryptography in Software,” 2012 Fourth International Conference on Multimedia Information Networking and Security, 2012, pp. 930-933, doi: 10.1109/MINES.2012.121.

[3] E. Jintcharadze and M. Iavich, ”Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems,” 2020 IEEE East- West Design Test Symposium (EWDTS), 2020, pp. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.

[4] Xinmiao Zhang and K. K. Parhi, ”High-speed VLSI architectures for the AES algorithm,” in IEEE Transactions on Very Large Scale Inte- gration (VLSI) Systems, vol. 12, no. 9, pp. 957-967, Sept. 2004, doi: 10.1109/TVLSI.2004.832943.

[5] Zou, Lin and Ni, Ming and Huang, Yiting and Shi, Wenfeng and Li, Xiaoxia. (2020). Hybrid Encryption Algorithm Based on AES and RSA in File Encryption. 10.1007/978-981-15-3250-4-68

[6] Khairnar, Dr. Vaishali and Kadam, K. (2015). Hybrid RSA-AES Encryp- tion for Web Service.

[7] E. Jintcharadze and M. Iavich, ”Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems,” 2020 IEEE East- West Design Test Symposium (EWDTS), 2020, pp. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.

[8] X. -h. Wu and X. -j. Ming, ”Research of the Database Encryption Technique Based on Hybrid Cryptography,” 2010 International Sympo- sium on Computational Intelligence and Design, 2010, pp. 68-71, doi: 10.1109/ISCID.2010.105.

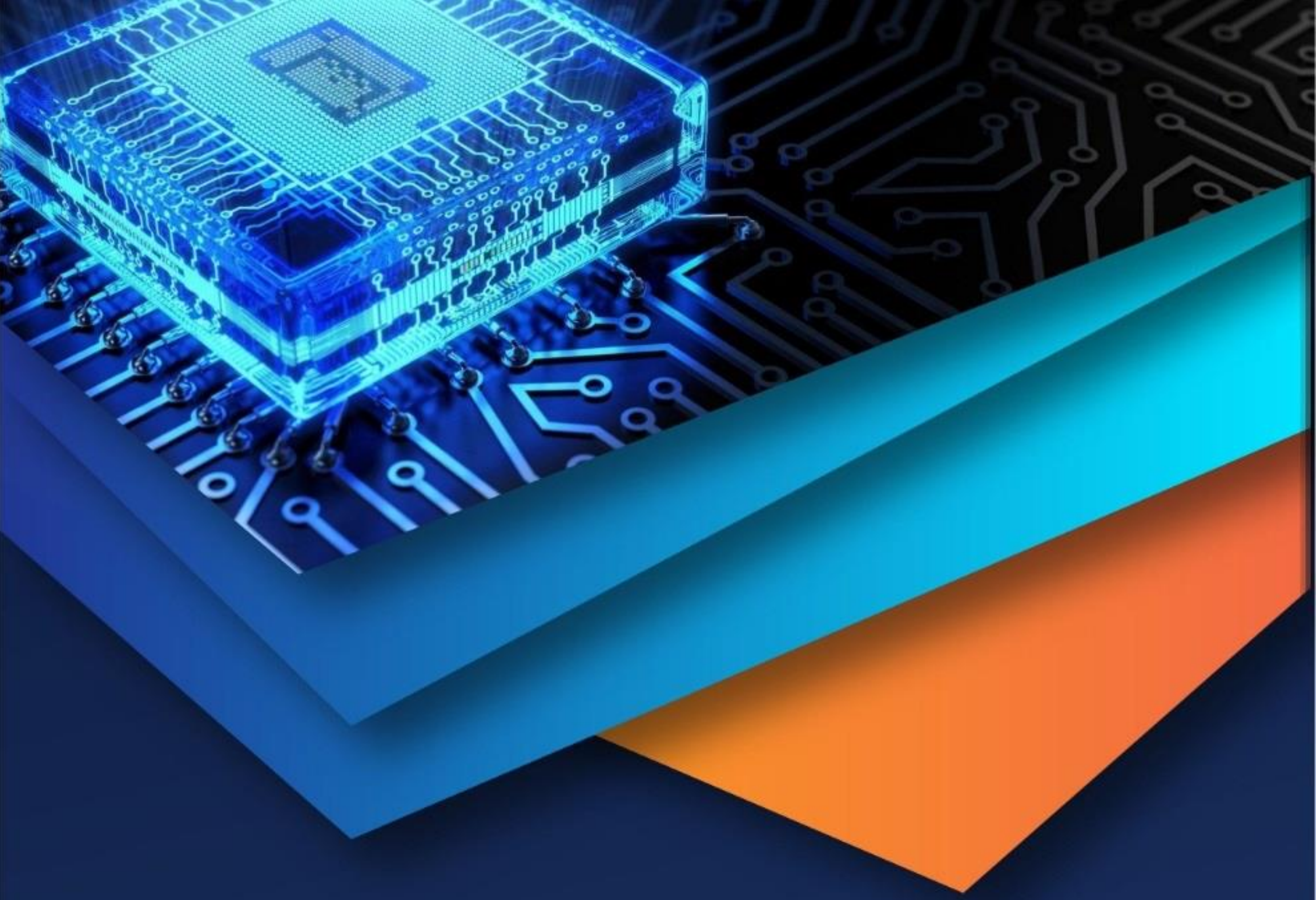
[9] S. K. Ghosh, S. Rana, A. Pansari, J. Hazra and S. Biswas, ”Hy- brid Cryptography Algorithm For Secure And Low Cost Communi- cation,” 2020 International Conference on Computer Science, Engi- neering and Applications (ICCSEA), 2020, pp. 1-5, doi: 10.1109/ICC- SEA49143.2020.9132862.

[10] D. P. Timothy and A. K. Santra, ”A hybrid cryptography algorithm for cloud computing security,” 2017 International conference on Micro- electronic Devices, Circuits and Systems (ICMDCS), 2017, pp. 1-5, doi: 10.1109/ICMDCS.2017.8211728.

[11] D. M. Alsaffar et al., ”Image Encryption Based on AES and RSAAlgorithms,” 2020 3rd International Conference on Computer Applica- tions and Information Security (ICCAIS), 2020, pp. 1-5, doi: 10.1109/IC- CAIS48893.2020.9096809.

[12] X. Zhang, M. Li and J. Hu, ”Optimization and Implementation of AES Algorithm Based on FPGA,” 2018 IEEE 4th International Conference on Computer and Communications (ICCC), 2018, pp. 2704-2709, doi: 10.1109/CompComm.2018.8780921.

[13] D. P. Timothy and A. K. Santra, ”A hybrid cryptography algorithm for cloud computing security,” 2017 International conference on Micro- electronic Devices, Circuits and Systems (ICMDCS), 2017, pp. 1-5, doi: 10.1109/ICMDCS.2017.8211728.



10.22214/IJRASET

INDEX COPERNICUS

45.98

ISRA JIF

IMPACT FACTOR: 7.129

SJIFactor

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

ISI

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY