Hybrid Cryptosystem to Securely Store Data

Rutuja Kale[1], Arati Manjaramkar[2]
[1,2]*Shri Guru Gobind Singhji Institute of Engineering and Technology Nanded, Maharashtra, India*

***Abstract*: In today's world, cloud computing is primarily used by private and public organizations for data storage and retrieval. Many organizations and end users can use cloud computing such as Google Drive, Amazon Web Services, and Microsoft Azure. Cloud computing and its services allow organizations/end users to store data. Enterprises face numerous challenges when storing sensitive data on cloud servers. So, these organizations need security and privacy to store data. This paper's goal is to present a high-level design for a storage system that maximizes security and user privacy. Combination of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) recommended for efficient cloud data storage security and integrity. The AES algorithm uses 256 bits key for providing enhanced security which is obtained through an optimized key generation module. The system development is done by using Apache PHP as a server-side technology to manage the encryption and decryption, user session handling and file management. User records are managed using MySQL relational database. The experimental finding demonstrates that security can be maximized by using a time-based one-time password, email address, mobile phone number, and password as the security criteria to verify against an intruder. The suggested solution is more effective in storing and retrieving huge amounts of data from a cloud server.**

Keywords: Cryptography, Decryption, Encryption, Security and Steganography

I. INTRODUCTION

The transmission of computing resources, including servers, software, networking, storage, databases, analytics, and intelligence through the Internet is known as cloud computing. This allows for quicker innovation, more adaptable resources, and larger markets. The development of cloud computing techniques led to the creation of vast, multifunctional facilities that are readily available and based on business requirements for comforts that support quick, effective results. It also provides with the ability to access corporate documents and shared infrastructure, provides on-demand services in network environments, and executes processes to meet growing business needs [1].

Cloud computing is defined as a collection of application software and services that can be deployed over the Internet rather than residing on local personal computers or local servers [2]. Similarly, [3] states that cloud computing is "a type of computing in which highly scalable and flexible IT capabilities are delivered as a service to remote customers using Internet technologies".

The security challenges attributed to cloud computing are enormous. Suppliers must therefore ensure that the facilities provided are safe. Cybersecurity has been identified as one of his top threats of today's world and has generated many concerns among individuals and cooperating organizations in cloud computing environment. Data theft continues to grow, reaching levels where organizations are finding new ways of data security that allow for secure data transfers, including information security [4].

In recent years, various applications based on cloud computing technology have emerged such as Remote storage, stock trading, utility payments. Such transactions over public wired or wireless networks required end-to-end secure connections and the exchange of information that must be confidential. To ensure data protection, businesses are realizing that they must integrate their critical business processes with the Internet to gain a competitive advantage.

Recent research in the field of e-business points to referring to the sensitivity level of information to build safe and efficient business processes integrated with various levels of security [5]. The idea of encryption help to increase the security of encrypted files uploaded on cloud storage. The essence is to ensure that files are encrypted and decrypted in a secure manner and in a very short time period with maximum cost efficiency. Running the process can prevent large-scale attacks on sensitive files [6].

II. RELATED WORK

According to Y Manjula, K B Shivakumar [9], the file is encrypted using AES, then divided into equal portions according to the number of cloud storage spaces available and stored as necessary. The data security provided by their proposed method is enhanced in a multi-cloud setting. However, their strategy is vulnerable to the transport layer middle layer man attack. Additionally, the solution is expensive because using many clouds for storage incurs additional costs, there is no authentication, and thus puts the approach in an unbalanced position.

According to Pasaribu, Hendra [10], file transfer over a network is vulnerable to security issues such data stealing by unauthorized users. In order to increase the value of data security, the author suggests combining the AES 256-bit method with the MD 5 hashing. But as of right now, MD5 cannot be considered a responsible option for a secure hash function.

According to Taha, Ali Abdulridha [11] created a novel hybrid cryptography method. They use plain text to test their suggested system. This is split into two segments and is being processed simultaneously while each segment is encrypted using a separate encryption technique. Given the use of an asymmetric cryptographic approach, the related cost would be extremely large.

By combining asymmetric (RSA), symmetric (AES), and SHA256 hash functions, another approach was developed by [12] to guarantee that the file meets the test of confidentiality, integrity, and authentication. However, RSA takes a long time to execute, and without an extra security layer, the validity of data containing SHA256 is called into question.

According to Ghoradkar, Sneha, and Aparna Shinde [13] use the Advanced Encryption Standard (AES) system, which uses three different secret key sizes with lengths of 128, 192, and 256 bits to encrypt images with a block size of 128 bits. The proposed architecture uses 256 key sizes and 128-bit blocks. The secret key, the yardstick that undermines security, and the intricacy of the algorithms are the author's main points of emphasis. However, the method is unauthenticated.

III. PROPOSED SYSTEM

The proposed hybridized method includes 256 bits key AES and DES. The proposed method consists of basically two design modules Encryption module and Decryption module.

A. ENCRYPTION MODULE

The Hybridized AES algorithm uses 256 bits key to providing security to data. Algorithm of encryption module as below:

A Hybrid Encryption Algorithm
Input : Original File (Plaine Text)
Output : Ciphertext
User Authentication(Username, Password)
START
File Upload (File, Encryption Key)
Split Operation (File, Number of Parts)
Hybrid Encryption Algorithm
Encryption Using AES (Part1, Key)
Function call(ARKey(),SByte(),SRow(),MCols());
Encrypted Part1 Stored on Disk
Encryption Using DES (Part2, Key)
Function call (IPermutation (),FPermutation ());
Encrypted Part2 Stored on Disk
END

Here,
IPermutation = Initial Permutation
FPermutation = Final Permuatation

B. DECRYPTION MODULE

The encrypted file is given as input to decryption module which can retrieved from the cloud server on successful authentication of the user. If user authentication fail then user is dismissed. The algorithm for decryption is as below:

B Hybrid Decryption Algorithm
Input : Ciphertext
Output : Original File (Plain Text)
User Authentication (Username, Password)
START
Call Download (File, Key);
Hybrid Decryption Algorithm
Decryption Using AES (Part1, Key)
Function call(MCols(),SRow(),SByte(),ARKey());
Decrypted Part1 Stored on Disk
Decryption Using DES (Part2, Key)
Function call(FPermutation(),IPermutation());
Merge (Part1, Part2)
Original File
END

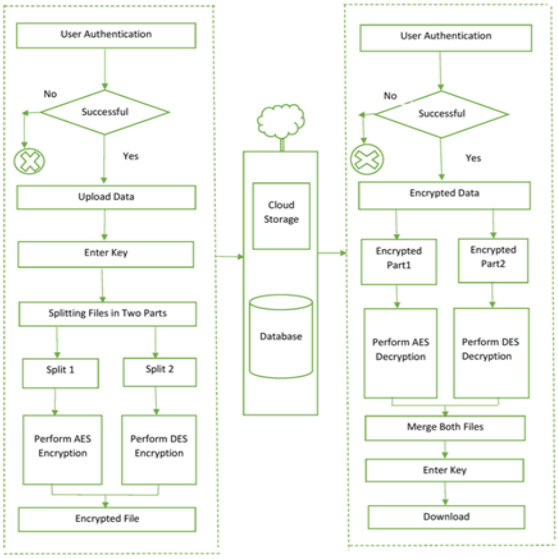

Fig 3.1: Hybridized Architecture

IV. RESULTS AND DISCUSSION

The proposed algorithm is hybrid, a combination of AES and DES algorithms it is implemented on Apache Server using Microsoft Visual Studio 2017 integrated development environment, it is tested with different input file (size varying from 1MB to 245MB). The output of hybrid algorithm is compared with output of AES and DES algorithm. The proposed hybrid system generates below results.

The output of the suggested hybrid system is shown in Table 4.1. This table records the file sizes for the AES, DES, and Hybrid systems before and after encryption. While the hybridized algorithm improves the size of the file by maintaining the original size, both AES and DES roughly double the encrypted file's original size. This is much better than when the encrypted file size is raised because there is no additional cost when uploading to the cloud server storage.

Table 4.1: EVALUATION OF FILE SIZE

AES		DES		Hybrid	
Default File Size (mb)	Encrypted File Size (mb)	Default File Size (mb)	Encrypted File Size (mb)	Default File Size (mb)	Encrypted File Size (mb)
1.00	1.84	1.00	2.00	1.00	1.00
10.00	19,59	10.00	20.00	10.00	10.00
20.00	39.54	20.00	40.00	20.00	20.00
40.00	79.69	40.00	80.00	40.00	40.00
55.00	109.80	55.00	110.00	55.00	55.00
75.00	149.49	75.00	150.00	75.00	75.00
110.00	219.99	110.00	220.00	110.00	110.00
120.00	239.70	120.00	240.00	120.00	120.00
160.00	319.90	160.00	320.00	160.00	160.00
170.00	339.30	170.00	340.00	170.00	170.00
200.00	398.81	200.00	400.00	200.00	200.00
245.00	489.76	245.00	490.00	245.00	245.00

The proposed ADK Hybrid was designed to efficiently upload big file sizes to cloud data storage.

Given the execution time, Hybrid performed much better than DES but significantly worse than AES for files smaller than 10MB.Figures 4.1 and 4.2 respectively, depict this clearly. The Hybrid performs substantially better from file sizes of 10MB and above, which is a plus. Amazingly, Hybrid outperforms both AES and DES, and the findings reveal that the bigger the file, the longer AES and DES take to execute.

Figure 4.1 depicts the execution timings for hybridized encryption and decryption. The findings demonstrate that both encryption and decryption have longer execution times. The time taken for encryption using the AES, DES, and Hybrid algorithms was compared in Figure 4.2. Hybrid performed remarkably well for File sizes start at 10MB and go up.

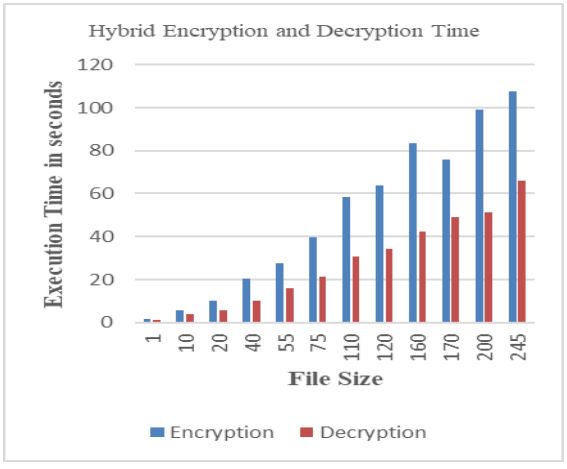

Fig 4.1 : Hybrid Execution Time

From above figure we can conclude that by using hybrid model we required less time for encrypting the data as compared to AES and DES algorithm.

Table 4.2: Execution Time of Respected Algorithms

File size (MB)	AES (seconds)		DES(seconds)		Hybrid(seconds)	
	Encryption	Decryption	Encryption	Decryption	Encryption	Decryption
1	1.564	1.429	3.085	2.010	3.049	1.575
10	5.702	4.061	7.305	4.993	4.795	1.890
20	10.222	5.863	11.583	8.028	6.636	2.296
40	20.269	10.024	22.750	13.603	9.278	2.976
55	27.706	15.799	30.833	19.559	10.844	3.759
75	39.788	21.260	38.913	25.010	15.220	4.815
110	58.334	30.544	46.092	38.401	30.578	6.727
120	63.76	34.151	62.735	45.830	21.097	7.019
160	83.626	42.460	110.528	45.446	27.413	9.482
170	75.648	49.081	118.172	46.722	28.996	9.306
200	99.070	51.063	126.592	55.971	33.156	10.684
245	107.572	65.896	147.278	90.619	40.109	12.979

Table 4.2 shows the execution time required for AES, DES, and Hybrid algorithm with test data of varying sizes.

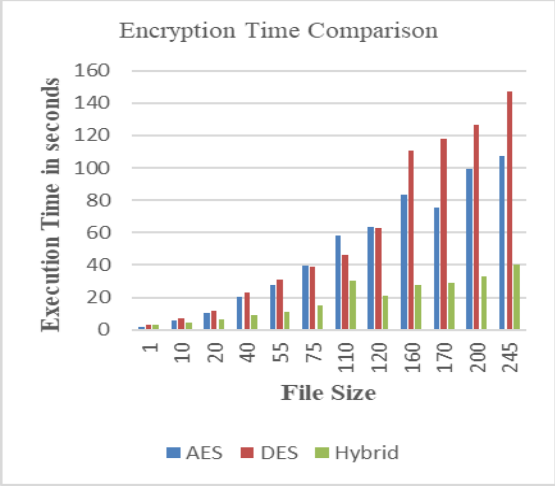

Fig 4.2: Encryption Time Comparison

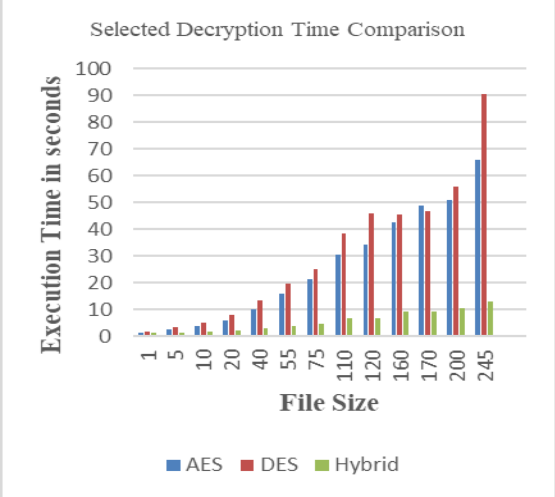

Fig 4.3: Decryption Time Comparison

Time required for decryption in Hybrid model is less as compared to AES and DES algorithm. So, using Hybrid model we can minimize the encryption and decryption time.

V. CONCLUSION

The issues of privacy and security of data is full of challenges. For improving data storage security continuous research is going on. This paper presents a Hybrid approach which is combination of AES and DES algorithm. By using this algorithm, large data files can be stored in a very secure environment. Because user is generating a key, that key is accessed by only authorized user. Since the proposed hybrid algorithm is implemented on cloud servers, data movement traffic is also minimized. In this research, the AES and DES algorithms are combined to provide an additional layer of security.

The proposed system is flexible which can assist to add number of algorithms encompassing encryption and decryption which can be applicable variety of commercial projects such as banking. The sequence of algorithm can also be used by variety of users. Ideally, this makes it cumbersome for an attacker to attack or decrypt plain input text unless they know the algorithms used in the encryption process, the order used, etc. Because the order is important for decoding. This flexibility allows them to be used in a wide variety of applications and also allows them to accommodate new algorithms developed in the future. Another innovative approach lets you specify passwords to help determine which algorithm to use from an array of them. When the software receives the

password and data, it calculates the algorithm and order of using based on the password, applies it to the data, and follows the during decryption.

REFERENCE

[1] Agrawal, Divyakant, Sudipto Das, and Amr El Abbadi. "Big data and cloud computing: current state and future opportunities." *Proceedings of the 14th international conference on extending database technology*. 2011.

[2] Stroh, S., O. Acker, and A. Kumar. "The Cloud is Ready for you, Are you ready for Cloud." *USA: Booz & Company. 9p* (2009).

[3] Gartner, T. Contributing factors of cloud computing adoption a Technology organization environment framework approach. International Journal of Information Systems and Engineering 1(1), pp.38–49.2012.

[4] Laney, Doug. "3D data management: Controlling data volume, velocity and variety." *META group research note* 6.70 (2001): 1.

[5] Chi, Sung-Do, et al. "Network security modeling and cyber-attack simulation methodology." *Australasian Conference on Information Security and Privacy*. Springer, Berlin, Heidelberg, 2001.

[6] Anjanachaudhary, ravinder Thakur, manishmann", A review: data security approach

[7] Cloud computing by using RSA algorithm", International Journal of Advance Research in Computer Science and Management Studies, volume 1,Issue 7, December 2013

[8] K. Yang, J. Xiaohua. Security for Cloud storage systems, Springer Brief in Computer Science, 2014.

[9] Y Manjula, K B Shivakumar. Enhanced Secure Image Steganography using Double Encryption Algorithms, at International Conference on Computing for Sustainable Global Development IEEE, 2016.

[10] Pasaribu, Hendra, et al. "Combination of advanced encryption standard 256 bits with md5 to secure a documents on android smartphone." Journal of Physics: Conference Series. Vol. 1007. No. 1. IOP Publishing, 2018.

[11] Taha, Ali Abdulridha, D. S. A. Elminaam, and Khalid M. Hosny. "An improved security schema for mobile cloud computing using hybrid cryptographic algorithms." Far East Journal of Electronics and Communications 18.4 (2018): 521-546.

[12] Aumasson, Jean-Philippe, et al. "BLAKE2: simpler, smaller, fast as MD5." InternationalConference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg, 2013.

[13] Ghoradkar, Sneha, and Aparna Shinde. "Review on image encryption and decryption using AES algorithm." International Journal of Computer Applications 975 (2015): 8887.

[14] V.Masthanamma,G.Lakshmi Preya "An Efficient Data Security in Cloud Computing Using the RSA Encryption Process Algorithm" 2015

[15] Ghavghave, Rashmi S., and Deepali M. Khatwar. "Architecture for data security in multicloud using AES-256 encryption algorithm." *International journal on recent and innovation trends in computing and communication* 3.5 (2015): 2321-8169.

[16] Walliman, Nicholas. *Research methods: The basics*. Routledge, 2010.

[17] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, ISBN 978-0-13-444428-4, Pearson Education, 2017.

[18] Taha, Ali Abdulridha, D. S. A. Elminaam, and Khalid M. Hosny. "An improved security schema for mobile cloud computing using hybrid cryptographic algorithms." *Far East Journal of Electronics and Communications* 18.4 (2018): 521-546.

[19] Clarke, R. J, Research Methodologies, Agenda Definition, 2005.

[20] S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." J Network ComputAppldoi:10.1016/j.jnca.2010.07.006. July, 2010

[21] Padmapriya, A., and P. Subhasri. "Cloud computing: security challenges and encryption practices." *International Journal of Advanced Research in Computer Science and Software Engineering* 3.3 (2013).

[22] Sneha Ghoradkar,Sneha Ghoradkar, "Review on Image Encryption and Decryption using AES Algorithm", 2015

[23] Peltier and Thomas, Designing information

security policies that get results. Info security news 4(2), 30-31. 1993.

[24] Akashdeep Bhardwaja, GVB Subrahmanyam , Vinay Avasthi, Hanumat Sastry ―Security algorithms for cloud computing‖, Procedia Computer Science, vol. 85, pp. 535-542, 2016.