IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 7.301

Volume 3, Issue 1, April 2023

The Design and Implementation of a Secure File Storage on the Cloud using Hybrid Cryptography

Gift Chisoni[1] and Dr. Glorindal Selvam[2]

Master of Computer Science, DMI-St. Eugene University, Zambia[1,2]

gchisoni@gmail.com[1] and glorygj@yahoo.com[2]

Abstract: *In recent years, cloud computing has become a popular way of storing and sharing data. However, security concerns have been raised about the safety of sensitive information stored on the cloud. Hybrid cryptography, which combines symmetric and asymmetric encryption, has been proposed as a solution to these concerns. This paper proposes a new hybrid cryptography approach for secure file storage on the cloud regardless of the type of deployment model i.e., either public cloud, private cloud, or hybrid cloud. The proposed approach uses a combination of the Advanced Encryption Standard (AES) algorithm, Triple Data Encryption Standard (DES) algorithm, and Rivest cipher 6 (RC6) algorithms are used to provide block-wise security to data. LSB steganography technique is introduced for key information security.*

Keywords: Hybrid Cryptography, Cloud Computing, Secure File Storage.

I. INTRODUCTION

Securing files on the cloud is a critical concern for individuals and organizations alike, as they want to ensure that their confidential information remains protected from unauthorized access. Hybrid cryptography is a security approach that combines the strengths of symmetric and asymmetric encryption to provide secure file storage on the cloud. Cloud computing originated from earlier large-scale distributed computing technology. The National Institute of Standards and Technology (NIST) defines Cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

Hybrid cryptography combines the strengths of both symmetric and asymmetric encryption. The data is first encrypted using a randomly generated symmetric key in this approach. The symmetric key is then encrypted using the receiver's public key, and both the encrypted data and encrypted symmetric key are stored in the cloud. When the receiver wants to access the data, they use their private key to decrypt the symmetric key and then use the decrypted symmetric key to decrypt the data.

The proposed system of using hybrid cryptographic system uses a combination of multiple cryptographic algorithms and steganography techniques. 3DES, RC6, and AES algorithms are used to ensure the security of data. The LSB steganography method is also implemented to store key information securely. The file is divided into three parts during the encryption process. Each part of the file will be encrypted using a dissimilar encryption algorithm simultaneously. After the encryption process, the key information is inserted into an image using the LSB method.

In summary, this proposed methodology ensures better security and safety of user data because DES alone is used for data encryption in financial transactions, electronic commerce, and other applications where high security is required. Additionally, it provides a stronger level of encryption than the original Data Encryption Standard (DES) algorithm. RC6 will be used because it is designed to be more efficient and faster than other block ciphers during encryption and decryption processes where high performance and flexibility are important. While AES is coming in because it is considered a highly secure algorithm and has become the de facto standard for encryption in many industries, including finance, healthcare, and government data.

DOI: 10.48175/IJARSCT-9067

II. RELATED WORK

Securing files on the cloud is an important topic, and hybrid cryptography is a popular technique for ensuring the security of cloud-based file storage systems. Security is an important factor in this digital age. So, a huge amount of research is conducted in this domain (cloud computing) to protect clients' information from any security breaches and leaks. There have been different scholars who have produced different security techniques to safeguard cloud information over time using cryptography. The following published articles have been referred to create a base for my project.

"Design of a Secure Virtual File Storage System on Cloud using Hybrid Cryptography". by Bello A. Buhari, Aliyu Mubarak, Bello A. Bodinga, and Muazu D. Sifawa (2022). in their research, [1] they introduced a Hybrid encryption algorithm cryptography method used for file encryption and decryption based on AES and SHA-2 hash functions. The proposed concept was implemented using Cloud APIs with REST calls or client libraries in PHP.

"Secure File Storage on Cloud Using Hybrid Cryptography" by Naveetha K. &T. Tamilarasan(2021). This paper [2] proposes a hybrid cryptography-based Attribute-based encryption (ABE). The purpose of this system was to provide fine-grained access control to encrypted data and provide a more flexible and secure approach to access control and data-sharing

"Secure data storage in cloud computing using hybrid cryptography" by K.R. Vinoth Kumar and K. Manivann, (2012). This paper [3] proposes a hybrid cryptography-based technique for secure data storage on the cloud. The proposed technique combines AES and RSA algorithms to encrypt and decrypt the data. The paper evaluates the performance of the proposed technique and shows that it provides secure data storage on the cloud.

"Performance comparison of data encryption algorithms" by A. Nadeem, (2006). A study in this paper [4] was conducted for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. The proposed system was implemented, and their performance was compared by encrypting input less of varying contents and sizes. In this paper, the algorithms were also tested on two different hardware platforms, to compare their performance.

"A Cloud Security using Hybrid Cryptography Algorithms " by Sanjeev Kuma, Garima Karnani, and Madhu Sharma Gaur (2021). This paper [5] proposes a hybrid cryptography-based scheme for secure data storage in cloud computing. The proposed scheme combines DES and RSA algorithms to encrypt and decrypt the data. The paper also evaluates the performance of the proposed scheme and shows that it provides secure data storage in cloud computing.

"A Secure File Storage on Cloud using Hybrid Cryptography " by A. Poduval1, A. Doke, H. Nemade, and R. Nikam (2019). [6] This paper proposes a hybrid cryptography-based approach for secure data storage in cloud computing. The approach uses DES, AES, and RC6 algorithms to encrypt and decrypt the data. The paper also presents the analysis of the proposed approach and shows that it provides secure data storage in cloud computing.

"Secure File Storage and File Sharing." by Rawal, B. S., & Vivek, S. S. (2017). This paper [7] proposes a cloud storage security service to be provided using separate servers. Three different servers are used to ensure that failure of any of the servers doesn't harm the data. In this paper, it was reviewed that the data storage server was used as a platform where the encryption using AES was performed to ensure user input and the encrypted files are transmitted to the User Output server.

"Secure file storage in cloud computing using a hybrid cryptography algorithm". By Punam V. Maitri, and Aruna Verma, (2016). The paper [8] focuses on how files are securely stored on a cloud platform. Furthermore, it discusses the problem of using only a single encryption algorithm to encrypt the file and how ineffective it will be on the cloud. This paper splits the file into blocks and each block is encrypted using AES, Blowfish, and RC6algorithm.

Rivest-Shamir-Adleman (RSA) Encryption and Digital Signature ". By Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). In this paper [9] the authors proposed a combination of the RSA and MD5 algorithm to assure various security procedures such as confidentiality, data integrity, non-repudiation, etc. RSA algorithms key is used for the generation of encrypted keys for encryption and decryption. MD5 is used for accepting an input of length up to 128 bits and processing it and generating an output of padded length for the encryption and decryption process.

"Use of Digital Signature with Diffie Hellman key exchange and AES encryption algorithm to enhance Data Security in Cloud Computing." By Rewagad, P., & Pawar, Y. (2013). [10] In this proposed system, a three-step procedure is used. Diffie Hellman is used for exchanging keys as the first step process. Authentication is performed using a digital

DOI: 10.48175/IJARSCT-9067

signature scheme as the second step process. And the last step, information is encrypted using AES and thereafter information is transferred to the required cloud system. For decryption, the reverse procedure is applied.

"Design and Implementation of Secure Cloud Storage System using Hybrid Cryptography Algorithms with Role-based Access Control Model" by Anjali DV, Dr. S.N Chandrashekara, (2016). This paper [11] describes the mathematical model for calculating the trust of the user by applying the cryptography concepts proposed by AES, RSA, and SHA-1 algorithm for encryption and decryption of data, and the role-based access control model is applied to provide access based on the role played by the user.

"Hybrid Cryptography for Secure Cloud Storage of Electronic Health Records" by V. Bharti and R. Sharma (2018). This paper [12] proposes a hybrid cryptography approach for secure cloud storage of electronic health records (EHRs). The system uses a combination of symmetric and asymmetric encryption, as well as digital signatures and MACs, to ensure the confidentiality, integrity, and authenticity of EHRs. The authors also evaluate the performance of their system using a real-world dataset.

In summary, based on the literature survey I conducted shows that hybrid cryptography is a promising solution for securing files on the cloud. The proposed techniques and schemes combine different symmetric encryption algorithms to ensure data confidentiality, integrity, and authenticity. These studies also evaluate the performance and security of the proposed approaches and show that they provide secure data storage in cloud computing.

III. METHODOLOGY

Algorithm to be used.

A. The Advanced Encryption Standard (AES) Algorithm

AES is a symmetric key block cipher used to encrypt data. It is currently one of the most widely used encryption algorithms and is considered highly secure. AES encrypts data in blocks of 128 bits and has key sizes of 128, 192, or 256 bits. It is used in many applications such as secure communication, electronic payments, and data storage.

B. Triple Data Encryption Standard (3DES) Algorithm

The Triple Data Encryption Standard (3DES) is a symmetric-key block cipher encryption algorithm. It is an improved version of the Data Encryption Standard (DES) and uses a key length of 168 bits (compared to 56 bits in DES) to provide stronger security. 3DES uses a combination of three individual 56-bit DES keys to provide a higher level of security.

C. 3DES Analysis

The DES satisfies both the desired properties of the block cipher. These two properties make the cipher very strong.

- Avalanche effect − A minor change in plaintext resulting in a major change in the ciphertext.
- Completeness − Each ciphertext bit relies on many bits of plaintext.

D. The Rivest Cipher 6 (RC6) Algorithm.

RC6 is one of the symmetric-key block ciphers that was developed by Ronald Rivest of RSA Security in 1998. It was designed to be efficient and secure, and it is widely used in a variety of applications, including encryption, authentication, and digital signature verification. One of the strengths of RC6 is its flexibility in terms of key length, block size, and the number of rounds.

E. Block cipher with a symmetric secret key

Key length	= from one byte up to 128 bytes
Block length	= 8 bytes

F. LSB (Least Significant Bit)

LSB is often used in digital signal processing, data compression, and encryption. In data compression, LSB manipulation involves changing the least significant bits of an image or audio file, which can reduce the file size

DOI: 10.48175/IJARSCT-9067

without significantly affecting its quality. In encryption, LSB steganography involves hiding secret data in the least significant bits of an image or audio file, which can help conceal the secret data's presence.

IV. PROPOSED SYSTEM

In this paper, AES, 3DES, and RC2 algorithms are used to provide block-wise security to data. LSB steganography technique is introduced for key information security. The file is fragmented into 3 parts. Each portion of the file is encrypted using a different algorithm. All parts of the file are encrypted at the same time with the help of the multithreading technique.

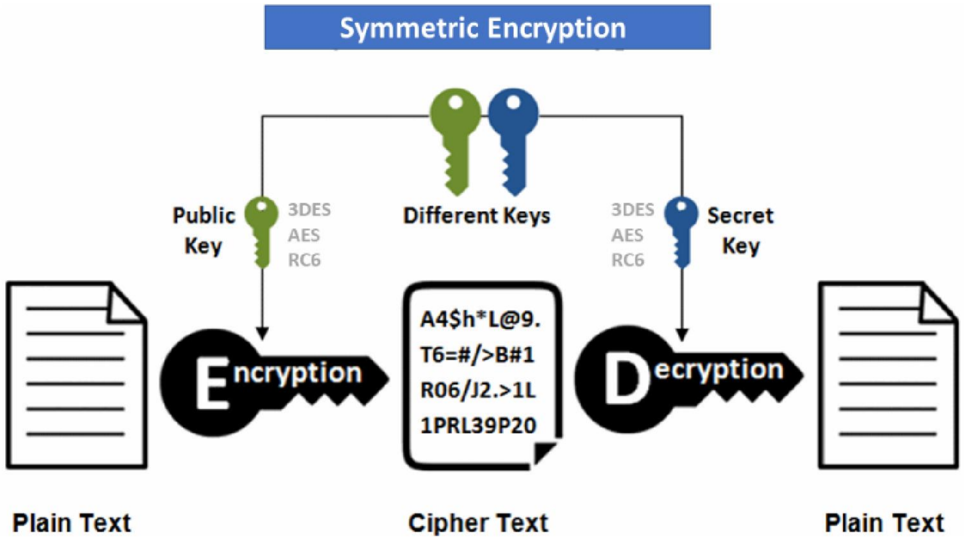

FIGURE 1: Encryption and decryption system model

The above diagram [figure 1] is an overview of the encryption process that has been adopted to implement the prototype. Referring the Figure 1, different public keys will be generated for the encryption process and the same process will be performed during the decryption. Meaning that three different keys will be used to decrypt the files.

The implementation of the proposed cryptographic system will involve developing a proof-of-concept prototype that will be used to evaluate the effectiveness of each algorithm. Furthermore, the prototype will be intended to simulate a cloud-based environment and will involve the use of a cloud server and a client to upload the files into the cloud. The system prototype will be developed using C# programming languages and their associated tools such as Visual Studio .NET framework and MS SQL.

Data encryption keys are inserted into a cover image using the LSB technique. Stego-Image is sent to a valid receiver using email. For file decryption purposes reverse process of encryption is applied. The files that the user will upload to the cloud system will be encrypted with a user-specific key and stored safely on the cloud. And in the same process, the recipient will receive an email containing a link where he/she can download a key which will be in a form of an image, and use it for the decryption process.

In summary, the proposed work in this paper is to design and implement a robust secure cloud storage system to achieve a higher level of security for file storage on the cloud using hybrid cryptography where the stored files are completely secured, as the files are being encrypted not by just using one but three encryption algorithms: AES, 3DES, and RC6. The performance of these algorithms can be evaluated on several factors including speed, security, and flexibility.

V. COMPARISON OF THE PROPOSED SYSTEM WITH SIMILAR WORKS

This section compares the proposed system which is the design and implementation of secure file storage on the cloud using hybrid cryptography with other reviewed works. The comparison is presented in tabular form as follows:

According to [Table 1] below, it provides a comparison of the proposed system with some related works and how this study is going to address some of the gaps.

Author & Year	Algorithm Used	Purpose of the system	Limitations
Sanjeev, Garima Karnani, & Madhu Gaur ***(2021)***	DES and RSA algorithms	The purpose of this system was to take advantage of the strengths of both algorithms to provide secure and efficient encryption in applications such as online banking, secure communications, and e-commerce	Vulnerability to brute force attacks. DES and RSA do not provide forward secrecy
Naveetha K. & T. Tamilarasan ***(2021)***	Attribute-based encryption (ABE)	The purpose of this system was to provide fine-grained access control to encrypted data and provide a more flexible and secure approach to access control and data sharing	It takes time for encryption, key generation, and decryption. The system is also restricted in the real-time environment
Bello A. Aliyu M. Muazu D.andBodinga ***(2022)***	AES and SHA-2 Hash Function	The purpose of this system was to provide strong security measures to protect sensitive data in various applications because AES is used for encryption, while SHA-2 is used for data integrity and authentication.	Less secure with many vulnerabilities Collisions are easy
*A. Poduval1, A. Doke, H. Nemade, and R. Nikam****(2019)***	DES, AES, and RC6	The purpose of this system wasto design an encryption algorithm for storing the secure file in multi-cloud storage andwireless communications, virtual private networks (VPNs), and other electronic data	The proposed system was prone to several security weaknesses
Proposed System	Design and implementation of secure file storage on the cloud using hybrid cryptography	3DES, RC6, and AES algorithms are utilized, and the key information will be encrypted using the LSB steganography method. Overall, the purpose of these proposed algorithms and LSB steganography technic is to ensure that sensitive data is protected from unauthorized access and interception during transmission or storage. The Least Significant Bit (LSB) steganography technic is coming in so that users should be able to hide sensitive data, such as passwords, and encryption keys within a digital image or audio file without visibly altering the original file.	

TABLE 1: Comparison of the proposed system with some related works

VI. DESIGN AND IMPLEMENTATION

The system prototype is designed in such a way that it has the following phases:

Register / Login:

- All users need to register first by filling up the basic registration fields.
- Using the combination of login id (email) and password, the user can log in to the system.

Upload Image:

- Here, different types of files to be stored are encrypted using **AES** (Advance Encryption Standard), **DES** (Data Encryption Standard), and **RC2** (Rivest Cipher 2) encryption algorithms.
- **LSB** (Least Significant Bit) steganography technique is introduced for key information security at this level.
- Key information contains which part of the file is encrypted using which algorithm and key.

Send a Message via Email:

- Once the encryption process has been completed in the background, this encrypted file is sent along with the image containing the key that is hidden in the image using LSB.

Download Image:

- Here, when the user request for a file to be downloaded, then that file is decrypted using AES, DES, and RC2.
- After successful decryption, the image file is merged into one file and then downloaded.
- The key is extracted from the image.

Log Generation:

- If the image file doesn't match the sender's image file, then the system will display a dummy file and the technical details such as user id, IP address, date, time, etc. will be stored in the database.

6.1 Proposed System Architecture

Overall, the proposed secure system architecture of hybrid cryptography is designed to provide a secure and efficient encryption scheme that combines the best features of cryptography. The system architecture diagram below simply explains the system as a whole and illustrates who is allowed to access the system and how they are going to access it.

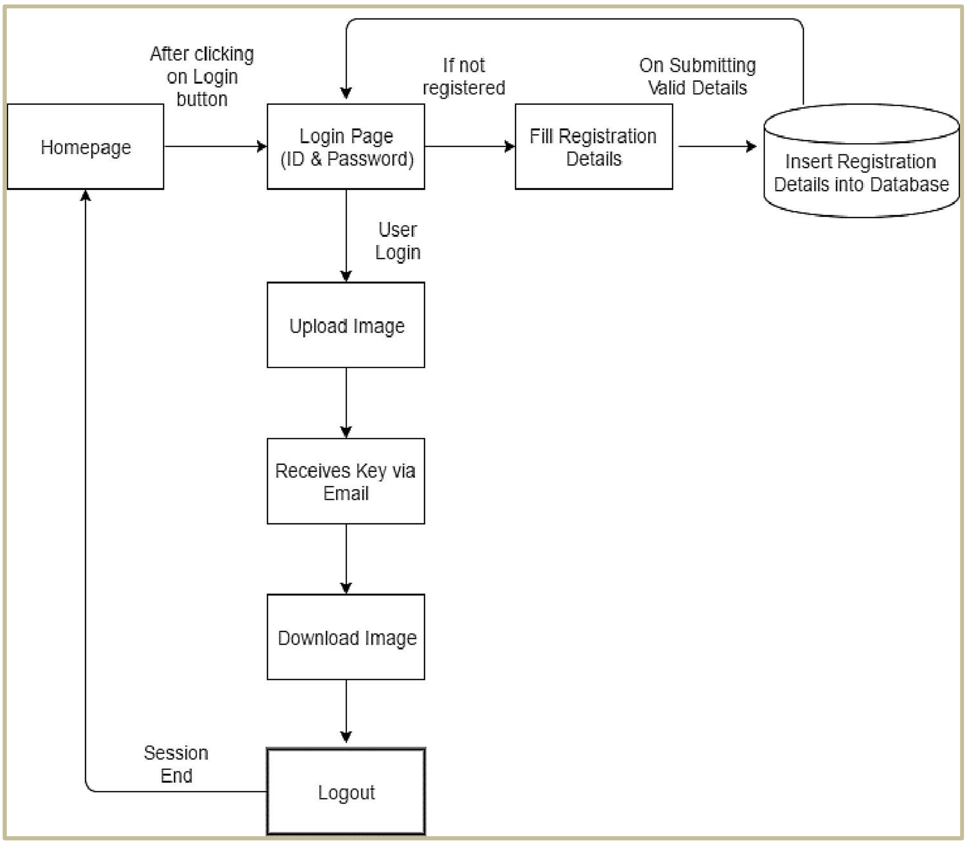
Homepage
After clicking on Login button
Login Page (ID & Password)
If not registered
Fill Registration Details
On Submitting Valid Details
Insert Registration Details into Database
User Login
Upload Image
Receives Key via Email
Download Image
Session End
Logout

FIGURE 2: Proposed system workflow

DOI: 10.48175/IJARSCT-9067

The diagram above [figure 2] simply explains how the system process works, that is from the user login process, upload files, generation of email notification, and the process of downloading the uploaded files from the cloud system.

VII. RESEARCH AND DISCUSSION

This paper proposes a design and implementation of secure file storage on the cloud using hybrid cryptosystems that provide a high level of security aside from maintaining confidentiality, usability, and scalability in cloud environments. A prototype will be developed to simulate the analysis of the proposed algorithms' performance measures and other metrics. The AES, 3DES, and RC6 are the symmetric-key encryption algorithms to be used because all three algorithms use a block cipher encryption method, meaning that they encrypt data in fixed-size blocks.

The results and performance of these algorithms were evaluated on several factors including speed, security, and flexibility.

- **Speed:** In terms of speed, AES has generally considered the fastest algorithm among the three. This is because AES uses a smaller block size (128 bits) than 3DES (64 bits) and RC6 (128 or 256 bits) and therefore requires less processing time. However, the key size of AES is larger (128, 192, or 256 bits) than DES (56 bits) and RC6 (128 or 256 bits), which means that AES requires more computation power than 3DES but less than RC6. DES is the slowest among the three algorithms due to its small block size and fixed key length.
- **Security:** In terms of security, AES is considered the most secure algorithm among the three. This is because AES has undergone extensive analysis and testing, and its security has been proven to be very strong. AES is also the only algorithm that is approved by the US government for use in securing classified information. 3DES, on the other hand, is considered less secure due to its small key size compared to AES. RC6 is considered secure, but it has not undergone as much analysis and testing as AES.
- **Flexibility:** In terms of flexibility, AES and RC6 are considered more flexible than 3DES. This is because AES and RC6 have variable key sizes, while 3DES has a fixed key size of 56 bits. AES also has three key sizes (128, 192, and 256 bits), while RC6 has two (128 and 256 bits). RC6 also has the added flexibility of being able to operate in both block cipher and stream cipher modes, making it useful for different encryption scenarios.

In summary, AES will be used as the primary encryption algorithm because of its efficiency and security while 3DES and RC6 will be used in combination with AES to provide additional security. AES is generally considered the fastest and most secure algorithm among the three, while RC6 is considered the most flexible. 3DES offers a high level of security but is relatively slower compared to other modern ciphers.

VIII. RESULTS AND DISCUSSION

8.1 Algorithm Evaluation - Speed

Based on the prototype simulation, the results of the proposed hybrid cryptography system for securing files on the cloud were evaluated using a series of tests. The system has been developed and implemented using asp.net. the system has a web interface that is used by end users for communication with the system. The tests were conducted to compare the proposed mechanism with the existing hybrid system.

Three text files (256KB, 512KB, 1MB, and 5MB) were used to achieve the three experimental results, and in each experiment, three cryptography algorithms (AES-256, 3DES-168, and RC6-128) were used. The Performance of each algorithm system was evaluated in areas of speed, memory file size, and throughput using *LabVIEW 2016 Simulation Program*.

DOI: 10.48175/IJARSCT-9067

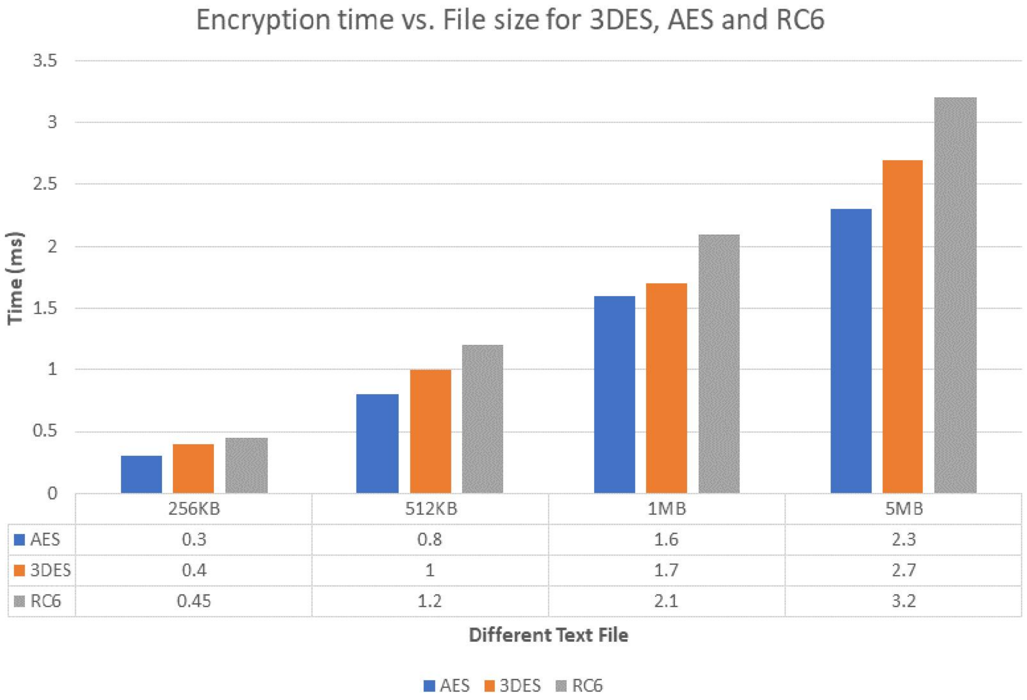

FIGURE 3: Performance comparison results of AES, 3DES, and RC6

Referring to the diagram above [figure 3], the figure simply explains the performance comparison results of each algorithm system after being evaluated in areas of speed, memory file size, and throughput. Four different file sizes were selected to evaluate the speed of encrypting and decrypting the selected sample files.

8.2 Algorithm Evaluation – Flexibility and Security

Based on the simulation, the results of the comparison of the three symmetric key encryption algorithms are presented in the table below [Table 2].

Symmetric Key Algorithm	Key Size (bits)	Number of Rounds	Block Size bits	Security	Speed
3DES	112, 1681	48	64	Very Good	Slow
AES	128, 192, 256	10, 12, 14	128	Excellent	Fast
RC6	128, 256	20, 26	32	Good	Fast

TABLE 2: Comparison of proposed algorithm evaluation

X. CONCLUSION AND FUTURE ENHANCEMENT

Hybrid cryptography is a powerful approach to secure file transfer on the cloud, combining the strengths of different encryptions. This approach uses a symmetric key to encrypt the file, which is then encrypted again with the recipient's public key, ensuring that only the intended recipient can decrypt the file.

While hybrid cryptography has been widely used in practice, there are still several gaps in research that need to be addressed in the future. Some potential areas for future research on hybrid cryptography include:

10. Gaps in Research Areas

- **Performance Optimization:** While hybrid cryptography is generally faster than asymmetric encryption alone, there is still room for improvement in terms of performance. Future research could explore new algorithms or techniques for improving the speed and efficiency of hybrid cryptography.

- **Standardization:** Hybrid cryptography is used in a variety of applications, from e-commerce to secure messaging to IoT devices. However, there is currently no standardized approach to hybrid cryptography, which can lead to interoperability issues and security vulnerabilities. Future research could focus on developing standardized protocols and algorithms for hybrid cryptography to promote interoperability and security.

Here are some potential future enhancements that could be made to strengthen the security offiles stored on the cloud system using hybrid cryptography:

- **Quantum-resistant algorithms:** With the coming of quantum computing, it's possible that some of the cryptographic algorithms currently used could be vulnerable to attack. As such, there is a need for quantum-resistant algorithms that can resist attacks from quantum computers. In the future, hybrid cryptography could incorporate these algorithms to provide even greater security.
- **Multi-party encryption:** In some scenarios, multiple parties may need to access a file, but ensuring that only authorized parties can decrypt it is important. Multi-party encryption could be achieved using hybrid cryptography by encrypting the file with multiple public keys so that each party can decrypt the file using their private key.
- **Use of blockchain:** Blockchain technology can be used to provide an immutable record of file transfers, which can be useful for auditing and compliance purposes. Hybrid cryptography could be combined with blockchain to create a secure and transparent file transfer system.
- **Integration with AI:** Artificial intelligence (AI) could be used to enhance the security of file transfers by detecting anomalies and potential threats. Hybrid cryptography could be integrated with AI to create a more advanced security system that can adapt to new threats and provide even greater protection.

Overall, hybrid cryptography is a promising area of research that offers many opportunities for future innovation and improvement. By addressing the gaps in the research outlined above, we can continue to enhance the security and efficiency of cryptographic systems and ensure that they remain robust and resilient in the face of emerging threats.

XI. ACKNOWLEDGMENT

I would like to express my sincere gratitude to all those who have supported me throughout this research endeavor. First and foremost, I would like to thank my supervisor, Dr.Glorindal Selvam, for providing me with guidance, encouragement, and constructive criticism at every step of the way. Her expertise and insights have been invaluable to me.

REFERENCES

[1]. Shrikanta Jogar1 & Darshan S Handral. (2022). “Secure File Storage on Cloud Using HybridCryptography”, International Journal of Advanced Research in Science, Communication and Technology (IJARSCT).

[2]. Gajanan T, S. Jayde, H.Gaurkhede, R. Vaidya, A.Wankhade& V.Yelekar. (2021). “Secure File Storage on Cloud Using Hybrid Cryptography”, International Research Journal of Engineering and Technology (IRJET). ISSN: 2395-0056.

[3]. M.Naveetha Krishnan&T.Tamilarasan. (2021). “Secure File Storage on Cloud UsingHybrid Cryptography”, International Journal of Advanced Research in Computer Science Engineering and Information Technology (IJARCSEIT).

[4]. Uttam Kumar, Mr. Jay Prakash. (2020). “Secure File Storage On Cloud Using Hybrid Cryptography Algorithm”, International Journal Of Creative Research Thoughts (IJCRT). ISSN:- 2320-2882 [Base Paper].

[5]. Aditya Poduval, Abhijeet Doke, Hitesh Nemade& Rohan Nikam. (2019). “Secure File Storage on Cloud using Hybrid Cryptography”, International Journal of Computer Sciences and Engineering (IJCSE).E-ISSN: 2347-2693.

[6]. M. Malarvizhi, J. Angela JennifaSujana, T.Revathi. (2014). “Secure File Sharing Using Cryptographic Techniques In Cloud”,International Conference On Green Computing Communication And Electrical Engineering (ICGCCEE).

DOI: 10.48175/IJARSCT-9067

[7]. Rawal, B. S., & Vivek, S. S. (2107). “Secure Cloud Storage and File Sharing”. IEEE International Conference on Smart Cloud (SmartCloud).

[8]. A. Buhari, A. Mubarak, B. Bodinga, and Muazu D. Sifawa. (2012). “Design of a Secure Virtual File Storage System on Cloud using Hybrid Cryptography”. Int. J. Advanced Networking and Applications

[9]. Maitri, P. V., & Verma. (2016). “Secure file storage in cloud computing using a hybrid cryptography algorithm”. International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),

[10]. Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). “RSA Encryption and Digital Signature”. (2011), International Conference on Computational and Information Sciences.

[11]. Rewagad, P., & Pawar, Y. (2013). “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing”.International Conference on Communication Systems and Network Technologies.

[12]. Anjali DV, Dr. S.N Chandrashekara. (2016). "Design and Implementation of Secure Cloud Storage System using Hybrid Cryptography Algorithms with Role-based Access Control Model", IJETR

[13]. Gajendra, B. P., Singh, V. K., & Sujeet, M. (2016). Achieving cloud security using third-party auditor, MD5, and identity-based encryption. 2016 International Conference on Computing, Communication, and Automation (ICCCA), 1304–1309.

[14]. Aman Kumar, Dr.Sudesh Jakhar, Mr. Sunil Makka. (2012). “Comparative Analysis between DES and RSA Algorithms”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2 Issue.

[15]. M. N Wahid, A. Ali, B. Esparham, M. Marwan. (2018).“Comparison of crypto. Algo: DES, 3DES, AES, RSA & blowfish for guessing attacks prevention” in 2018 Comp Sci Appl Techno.

[16]. Ashish Sharma, Dinesh Bhuriya, Upendra. (2017). Singh Survey of stock market prediction using machine learning approach “International conference of Electronics, Communication and Aerospace Technology (ICECA)”.

[17]. Mr. Gajanan N. Tikhe, Mr. Jeetendra Ambulkar. (2011). “A Certificate-Based Scheme to Defend against Wormhole Attacks in Ant-based Adaptive Multicast Routing Protocol for MANET”, in ICCCT, Delhi

[18]. Mr. Gajanan N. Tikhe, Mr. Yogadhar Pandey. (2012) “A Secure Scheme to Avoid Wormhole Attacks in Ant-based Adaptive Multicast Routing Protocol for MANET”, IFRSA’s International Journal Of Computing (IIJC) Volume 2, Issue 1, ISSN (Print):2231:2153, ISSN (Online):2230:9039

[19]. Dan Dobre, Paolo Viotti, Marko Vukolic. (2017). " Hybris: Robust Hybrid Cloud Storage", ACM Transactions on Storage, Vol . 13, Issue 3, October 2017

[20]. Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient Data Security Using Hybrid Cryptography on Cloud Computing.

[21]. Kumar, A., Lee, B. G., Lee, H., & Kumari. (2012).“Secure storage and access of data in cloud computing”. International Conference on ICT Convergence (ICTC).

[22]. A. Nadeem. (2006). “A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, pp. 84-89.

DOI: 10.48175/IJARSCT-9067