Secured File Sharing Through Quantum Computing

Ananya V[1], Apeksha S Kenchareddy[1], Dhanushree S P[1], Praveen S[1], Ms. Gagana G R Nayaka[2]

[1]UG Students, Department of Computer Science and Engineering, PESITM, Shimoga

[2]Assistant Professor, Department of Computer Science and Engineering, PESITM, Shimoga

NH – 206, Sagar Road, Shimoga Dist., 577 204, Karnataka, India.

Email: {anuananya46442 , apekshaskenchareddy, dhanushree.1516 , praveens.7349}@gmail.com, gaganagr@pestrust.edu.in

***ABSTRACT*- In present technology, Quantum computing plays a versatile role in data security and privacy. There are many methods for securing the data one of the methods is cryptography. File encryption and decryption become easier when the AES and RSA algorithms improve security. Also, file sharing through the AWS cloud and downloading from it have become more secure for storing data. Here we can add files into images with the help of Stenography. The comparison among the AES and RSA algorithms of performance speed, key size, and bit size is evaluated. In this paper, we proposed a framework for quantum key-based embedding and de-embedding of files and images where security and privacy are achieved. Access IBM server gives us Quantum processing units(QPUs) that are ibm_sherbrooke, ibm_kyiv, and ibm_brisbane. It requires a total of 127 Qubits and 30K CLOPS.**

Keywords-AES, RSA, Cryptography, Stenography, AWS Cloud, IBM Server

I. INTRODUCTION

Quantum computing is emerging as a transformative technology with the potential to revolutionize data security and privacy. As cyber threats become more sophisticated, the demand for secure methods of data protection is greater than ever. Cryptography has long been a cornerstone in securing sensitive information, with algorithms like AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) offering robust encryption and decryption capabilities. These algorithms are widely used to protect data during transmission and storage, ensuring confidentiality and integrity. However, with the advent of quantum computing, traditional cryptographic methods face challenges, necessitating the integration of quantum-enhanced techniques for improved security. Cloud platforms such as AWS have become integral for file storage and sharing due to their scalability and accessibility. Nevertheless, ensuring the privacy of files stored in the cloud remains a priority. This study addresses this issue by incorporating steganography techniques to embed files into images, adding another layer of security. Steganography not only conceals data but also makes it imperceptible, making it a complementary approach to cryptographic methods. Additionally, the research evaluates the performance of AES and RSA algorithms in terms of processing speed, key size, and bit size to identify their strengths and limitations in securing file-sharing processes. The proposed framework takes security to the next level by integrating quantum key distribution (QKD) for embedding and de-embedding files and images.

Fig.1:Typical Data Encryption Key Security

QKD leverages the principles of quantum mechanics to create encryption keys that are immune to interception, ensuring unparalleled security. Access to IBM's quantum processing units (QPUs)—including IBM Sherbrooke, IBM Kyiv, and IBM Brisbane—enables the implementation of this framework. These QPUs provide 127 qubits and 30K CLOPS (Circuit Layer Operations Per Second), offering the computational power necessary to support quantumbased security operations.This paper introduces a comprehensive framework that combines quantum computing, cryptography, and steganography to enhance data security in file-sharing applications. The proposed solution addresses contemporary a secure, scalable, and efficient method for protecting sensitive information stored and shared in cloud environments.

II LITERATURE REVIEW

Cryptography and steganography are well-researched areas aimed at enhancing data security. Over the years, various studies have examined the effectiveness of different encryption algorithms and steganographic methods in protecting sensitive information.

The Advanced Encryption Standard (AES) has been a prominent choice in data encryption, as highlighted in several studies. Padate and Pattel (2014) presented AES as a reliable algorithm for encrypting and decrypting text, emphasizing its simplicity and robustness in ensuring data confidentiality [1].

Similarly, Abdullah (2017) explored AES in applied mathematics and computer science contexts, discussing its advantages in encrypting data for enhanced security [2]. Silva and Heriyanto (2013) implemented AES encryption and decryption on Android operating systems, showcasing its practical application in mobile environments [3]. Furthermore, Ilyas and Widodo (2014) extended AES with a dual-password mechanism, demonstrating improved security for file encryption [4].

Incorporating steganography alongside encryption has been a popular approach to secure data. Rahmawati and Rahardjo (2016) combined AES encryption with the Discrete Cosine Transform (DCT)-based steganography to secure data in educational settings, offering dual-layer protection [5]. Bhaudhayana and Widiartha (2015) implemented AES-256 encryption with the Least Significant Bit (LSB) steganography method on bitmap images, achieving robust image-based security [6]. Krikor et al. (2009) further demonstrated the effectiveness of DCT in image encryption, showing its ability to integrate seamlessly with cryptographic techniques [7].

Selective encryption has also been extensively studied, particularly in the context of multimedia and images. Pommer and Uhl (2003) proposed selective encryption methods for waveletpacket encoded image data, balancing efficiency and security [9]. Abdmouleh et al. (2017) introduced a selective encryption algorithm based on Discrete Wavelet Transform (DWT), specifically targeting medical images to ensure privacy without compromising image quality [10].

Qiu et al. (2015) developed fast selective encryption methods for bitmap images, focusing on computational efficiency in data protection [12]. Shahid and Puech (2013) explored visual protection in HEVC video using selective encryption of CABAC bin strings, which proved effective for multimedia security [13].

Quantum computing has emerged as a game-changing technology in secure communications. Li et al. (2017) introduced intelligent cryptographic approaches for secure distributed big data storage in cloud computing environments, leveraging the capabilities of quantum cryptography to enhance traditional security measures [15]. The integration of quantum mechanics in encryption algorithms has further strengthened data protection frameworks, providing a foundation for addressing emerging cybersecurity challenges.

The Literature review gives some highlights of the extensive research on cryptography, steganography, encryption, and decryption techniques, as well as the adoption of quantum computing in enhancing data security and privacy. The integration of AES and RSA with steganography and the application of quantum computing

principles provide a robust framework for the secure communication of information through the cloud. Building upon these advancements, this research proposes a novel approach to combine quantum key-based encryption with steganographic embedding to ensure comprehensive security for file-sharing systems.

III. SYSTEM OVERVIEW

The system ensures secure communication between a sender and a receiver by combining compression, encryption, and steganography techniques. Firstly, the sender sends a plain text message, which is compressed to reduce its size, optimizing data transfer efficiency. The compressed data is then encrypted using a cryptographic algorithm such as AES or RSA, along with a secret key, ensuring that the message remains secure and inaccessible to unauthorized parties. Following encryption, the data is embedded into a cover media, such as an image, using steganographic techniques. This process conceals the encrypted message within the media, producing a stego-media file that appears inconspicuous. A stego-key is also generated, which is required to extract the hidden data on the receiver's side.

The stego-media file is transmitted over a communication channel, where a warden may observe the media but cannot detect the presence of sensitive information due to the steganographic embedding. Upon reaching the receiver, the stego-media is processed to extract the hidden data using the stego-key. The extracted data is then decrypted with the appropriate cryptographic key to restore the original compressed message. Finally, the decrypted data undergoes decompression to reconstruct the original plain text message for the receiver.

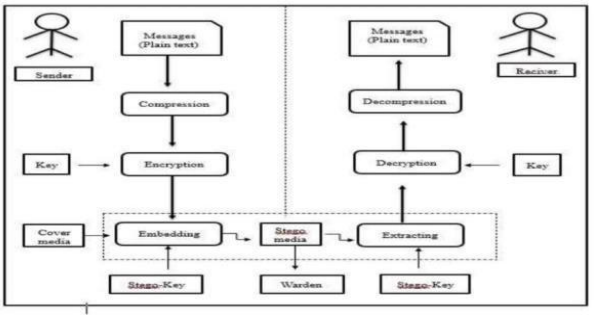

Fig.2: Architectural diagram for Encryption and Decryption.

This system provides robust security by integrating multiple layers of protection. Compression improves efficiency, encryption ensures data confidentiality, and steganography enhances privacy by making the hidden data imperceptible. The use of a stego-key adds another layer of control, ensuring only authorized users can access the embedded information. Together, these features make the system highly secure and reliable for transmitting sensitive data.

IV. METHODOLOGY

The project utilizes quantum computing and classical cryptographic methods to ensure secure file sharing and encryption. A user-friendly interface is created using Tkinter, allowing users to interact with various functionalities, including file encryption, hiding images in text, sending emails, and viewing contact information. The project employs Qiskit, a quantum computing library, to integrate the BB84 quantum key distribution (QKD) protocol, which generates a secure encryption key. This key is used with AES encryption in CBC mode to encrypt files, ensuring data security. The GUI enables easy navigation through these processes, making it accessible for users to securely encrypt and share files.

In addition to the user interface, the project connects to IBM's quantum service using Qiskit Runtime Service, allowing the execution of quantum algorithms in the cloud. The quantum key is generated by running a quantum circuit based on the BB84 protocol, which is simulated to produce the encryption key. Once the key is generated, it is used to

encrypt files securely. The project combines quantum key distribution with classical encryption techniques to enhance security, offering a hybrid solution for safe file sharing and encryption.

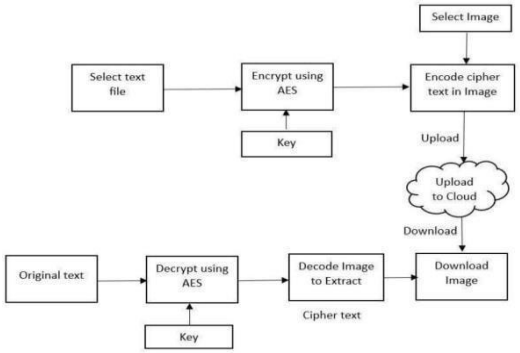

Fig.3: State diagram for AES algorithm

V. RESULT ANALYSIS

The comparison shows that AES encryption (0.02 seconds) takes longer than RSA encryption (0.006 seconds) and decryption (0.0018 seconds), highlighting their differing use cases. AES, with its block-based processing, is suitable for encrypting large data volumes due to its high security and throughput, while RSA's faster encryption and decryption make it ideal for secure key exchanges or small data payloads. The faster RSA decryption enhances its practicality in scenarios requiring frequent access to encrypted data.

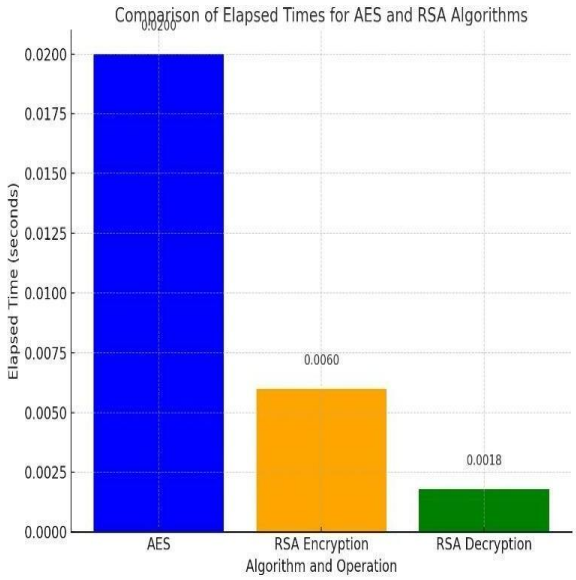

Fig.4: Comparison of Elapsed Time For AES and RSA Algorithms.

VI. CONCLUSION

The project demonstrates the integration of quantum computing with classical encryption methods for secure file sharing. By utilizing Qiskit and IBM's quantum service, it generates encryption keys using the BB84 quantum key distribution protocol, enhancing the security of encrypted files. The userfriendly Tkinter interface allows seamless interaction, making it accessible for users to encrypt files and manage encryption tasks easily. This approach showcases the potential of combining quantum technologies with traditional cryptographic algorithms like AES to address emerging cybersecurity challenges, offering a promising solution for the future of secure digital communication.

REFERENCES

[1] R. Padate, and A. Pattel, “Encryption and Decryption OfText Using Aes Algorithm,” International Journal Of Emerging Technology And Advanced Engineering, 2014.

[2] A. M. Abdullah, “Advanced Encryption Standard (AES)Algorithm to Encrypt and Decrypt Data,” Research Gate Departement Of Applied Mathematics & Computer Science, Cyprus UK. 2017.

[3] L. D. Silva and D. B. P. Heriyanto, “Aplikasi Enkripsi dan dekripsi file dengan Menggunakan AES Algoritma Rijndael Pada Sistem Operasi Android ,”JurnalTELEMATIKA Universitas Pembangunan Nasional “Veteran”.

[4] I. A. Ilyas and S. Widodo, “Kriptografi File Menggunakan Metode AES Dual Password,” Prosiding Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2014) Universitas Gunadarma .

[5] R. Rahmawati and D. Rahardjo, “Aplikasi PengamananData Menggunakan Algoritma Steganografi Discrete Cosine Transform dan Kriptografi AES 128 BIT pada SMK PGRI 15 Jakarta,” Jurnal Teknik Informatika dan Sistem

Informasi Vol. 2 No. 1 April 2016 e-ISSN : 24432229 Hal. 67 – 74.

[6] G. W. Bhaudhayana and I. M. Widiartha, "ImplementasiAlgoritma Kriptografi Aes 256 Dan Metode Steganografi Lsb Pada Gambar Bitmap,"Jurnal Ilmiah Ilmu Komputer Univetsitas Udayana Vol. 8 No. 2 September 2015.ISSN 1979-5661 halaman 15-25.

[7] Krikor, Lala, et al. "Image encryption using DCT and stream cipher." European Journal of Scientific Research 32.1 (2009): 47-57.

[8] H.Qiu,G.Memmi,X.Chen,andJ.Xiong,"DCcoeffici entrec overy for JPEG images in ubiquitous communication systems," Future Generation Computer Systems,2019.

[9] Pommer, Andreas, and Andreas Uhl. "Selective encryption of wavelet-packet encoded image data: efficiency and security." Multimedia Systems 9.3 (2003): 279-287.

[10] Abdmouleh, Med Karim, Ali Khalfallah, and Med Salim Bouhlel. "A novel selective encryption DWT-based algorithm for medical images." 2017 14th International Conference on computer Graphics, Imaging and Visualization.IEEE,2017.

[11] Gai, Keke, et al. "Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks." IEEE transactions on Smart Grid 8.5 (2017): 2431-2439.

[12] Qiu, Han, and Gerard Memmi. "Fast selective encryption methods for bitmap images." International Journal of Multimedia Data Engineering and Management (IJMDEM)6.3(2015):51-69.

[13] Shahid, Zafar, and William Puech. "Visual protection of HEVC video by selective encryption of CABAC bin strings." ieee transactions on multimedia 16.1 (2013): 24-36.

[14] Xiang, Tao, Chenyun Yu, and Fei Chen. "Secure MQ coder: An efficient way to protect JPEG 2000 images in wireless multimedia sensor networks." Signal Processing: Image Communication 29.9 (2014): 1015-1027.

[15] Li, Yibin, et al. "Intelligent cryptography approach for secure distributed big data storage in cloud computing." Information Sciences 387 (2017): 103-115.