ISSN: 2093-5374 / E-ISSN: 2093-5382

Secure Framework Optimizes QAES Technique Used for Computing in the Cloud

E. Geetha Rani[1*], and Dr. Chetana D. Tukkoji[2]

[1*]Research Scholar, Department of Computer Engineering, GITAM University, Bengaluru, India.
grani@gitam.in, https://orcid.org/0000-0002-4993-3923

[2]Assistant Professor, Department of Computer Engineering, GITAM University, Bengaluru, India.
ctukkoji@gitam.edu, https://orcid.org/0000-0002-1332-1466

Received: May 22, 2024; Revised: July 28, 2024; Accepted: August 26, 2024; Published: September 30, 2024

Abstract

Several consumers are concerned about the security of their data kept in the cloud, and many see local servers as a safer choice due to perceived control. However, cloud service companies frequently promise greater security procedures and employ dedicated security specialists, making data stored in the cloud potentially more secure. When the data holder expires, new files are saved in the cloud and encrypted with the QAES technology. The data owner then receives the encrypted data request. The sender and user both analyze data before sending encoded documents to the cloud. The key will be used to remove encryption from subsequent data. If users are unable to access the desired data, they should submit a fresh request. The most recent innovation focuses on combining an enhanced form of Quantum Key Distribution (QKD) with AES. This integration resulted in Quantum-AES (QAES), a novel quantum symmetric encryption scheme. QAES is based on the development of a quantum encryption key using dynamic quantum S-Boxes (DQS-Boxes), as opposed to the frequently utilized static S-Boxes. This strategy enhances security. Comparably, time is required to build files faster than they do now. This approach prevents brute force attacks since it uses the QAES algorithm, which provides additional security.

Keywords: Data Security, Encryption, QAES, Access Control, Cloud Computing, Decryption, AWS and CSP.

1 Introduction

You're putting cloud data security into practice when you use technological options, rules, then strategies to safeguard associated cloud-based systems, data, applications, and user access. The essential principles of data governance and information security more especially, data confidentiality, integrity, and availability trinity apply to cloud computing as well. Protecting the data from unauthorized Confidentiality is defined as being accessible and disclosed. Integrity: keeping the data from undergoing unauthorized alterations so that it may be relied upon. ensuring that data is fully available and ready to use as needed. Regardless of the cloud service type you use public, private, hybrid, or community these guidelines still hold (Neelima et al., 2024). Data security must constantly be considered when accessing the cloud, controlling the cloud infrastructure, and developing, deploying, or migrating applications and

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 15, number: 3 (September), pp. 312-324. DOI: *10.58346/JOWUA.2024.I3.021*

*Corresponding author: Research Scholar, Department of Computer Engineering, GITAM University, Bengaluru, India.

systems. A basic cryptography Strength is measured by how well it keeps secrets. They continue to be often sent stylish pieces with n- bit security meaning the adversary needs to carry out actions before breaking it. Despite its imperfections, it makes the process evaluation simple. The essential principles of data governance and information security more especially, data confidentiality, integrity, and availability trinity apply to cloud computing as well. protecting the data from unauthorized Confidentiality is defined as being accessible and disclosed. Integrity: keeping the data from being altered without authorization so that it may be relied upon. ensuring that data is fully available and ready to use as needed. These guidelines are relevant Whether you utilize clouds that are community, private, hybrid, or public, there are cloud services available. Data security must constantly be considered when accessing cloud computing, cloud environment management, and developing, deploying, or migrating applications and systems (Malathi, 2024). Despite its imperfections, it makes the process evaluation simple. AES-256 and AES-128 require roughly 2256 keys each, with a key size of 128 bits. The same seek might be completed by a quantum processor using just 2128 keys. That is substantially faster, to be sure. Should the length of the key surpass hybrid or community? Data security must constantly be considered Taking care of the cloud environment when utilizing it, and developing, deploying, or migrating applications and systems (Sonya & Kavitha, 2022). Cryptographic primitive strength is measured by how smoothly it keeps secrets. They continue to be commonly sent using bits, with n-bit safety meaning the adversary needs to carry out operations right before bleaching it. Despite its imperfections, it makes the process evaluation simple. AES-256 and AES-128 (key size 128 bits) require approximately 2256 keys. The same seek might be completed by a quantum processor using just 2128 keys. That is substantially faster, to be sure. However, there is still a lot to do. Larger key sizes are needed for quadratic speedup to make up for this. The prevailing consensus is that AES-like ciphers are quantum-safe when the length of the key exceeds 256 bits. Figure 1 shows that the structure of substitution boxes and several rounds, or S-boxes, in the conventional AES, is covered and analyzed in this work. Furthermore, DQS-Boxes, or dynamic quantum S-Boxes are constructed based on a quantum encryption key. At last, QKD and an improved version of AES are integrated to create a new version of AES.

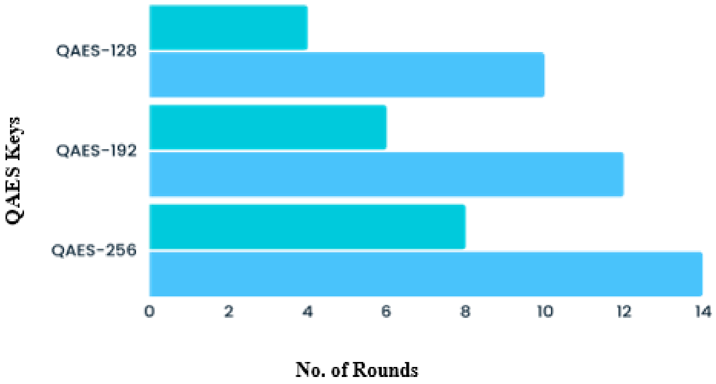

Figure 1: No. of Rounds Vs QAES Key

2 Related Works and Contribution

Traditional Cryptography

A Cryptographic Cloud Computing The surroundings are a More Trusted Communication setting. This publication's author suggested a revised security architecture that considers every major security vulnerability in the cloud computing environment. For cloud security, an algorithm for hybrid RSA encryption is being developed. The three services that are Among services are infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS) offered by clouds (Shiraishi et al., 2011). system provides its users with (IaaS). With a cloud system, data is processed, moved between clients and servers, stored on servers, and handled. For this reason, data needs to be protected while it is on the server, as well as throughout its movement across the network. Maximum Security is a difficult problem while employing cloud computing, a new technology (Harnoš & Dedera, 2021). Should the attacker manage to gain public key value; the comparatively antiquated RSA security technique might not be able to protect information while it is being transported. Attacks by a man in the middle can be prevented by implementing this recommended hybrid encryption using the RSA technique for cloud systems' data transfer for cloud systems' data transfer (Kholod et al., 2020). The developers of attribute-based ciphertext-policy encryption are Waters and Bethencourt J. Sahai. The purpose of this work is to address this problem and provide the first ciphertext-policy encryption based on attributes (CP-ABE) design (Sriram, 2022). The private key of an individual in our system will be associated with any number of strings that stand for attributes. In contrast, when parties encrypt a message using our technology, they declare a connected access structure over characteristics. A user's characteristics must transit through the ciphertext's access structure for them to be able to decode the data. From a mathematical standpoint, the structure of the system's access can be represented as a monotonous "access tree," with nodes standing in for leaves and threshold gates in terms of attributes (Ouda et al., 2022). We observe that gates that are for example, between n and 1 threshold gates out of a total of n, Moreover and OR can be constructed. Even more intricate access controls, such as numeric ranges, can be managed by converting them into tiny access trees. The original text is converted into ciphertext using classical coding, and it is then transmitted over an important data string-manipulated channel (Tukkoji, 2024). The recipient can only access original data and decode original text if they possess this key. Symmetric and asymmetric cryptography are the two categories under which classical cryptography falls. These cryptographic methods are threatened by quantum algorithms, though. Furthermore, the security of conventional cryptography is threatened by advancements in quantum computing, CPU power increases, new attack techniques, and vulnerable accidental key originators (Korać et al., 2022). Quantum computers negate the use of such encryption. Encrypted data can now be recorded and gathered for decryption by quantum computers in the future.

Quantum Cryptography

Using machines to generate keys chosen at random in this novel setting, the algorithm for QKD, or key distribution, and AES, or advanced encryption standard method are coupled to provide the principal security algorithm that is applied to both encryption and decryption operations. By identifying attacks, The QKD process offers communication parties greater freedom because it is based on random key generation. Recognized as the cloud computing hybrid pioneer, its primary focus is on two issues: short distance and key availability, which are connected to QKD and AES, respectively. Rajbir and Manpreet, boosting Data Security in Cloud Computing with Encryption Algorithms. Cipher cloud architecture enables users to protect the privacy of their data on open cloud services (Korać et al., 2022). To achieve this, Cipher Cloud utilizes a two-phase encryption method. process that guarantees total secrecy of any information sent to a client via a cloud server, or vice versa (Leung et al., 2020). Even when they occasionally understand the most popular private cloud computing designs, using public cloud infrastructures may not guarantee the extensive security measures needed to secure the most private information (Tukkoji, 2024; Albert Carlson et al., 2022; Rawat et al., 2023). The most effective method for cloud computing, which almost ensures data security like private cloud models, is recommended by this article to be selective encryption methods (Jabber et al., 2023). A system that safeguards the distribution of quantum-resistant symmetric encryption keys mechanical concepts is referred to as quantum cryptography (Brotherton & Gupta, 2023). More precisely, it's called quantum key distribution (QKD). It uses an optical network to transfer light's "quantum particles," or photons. Any observation of a quantum state will disrupt it, according to the fundamentals of quantum physics. The goal of the several QKD methods is to guarantee that any person trying to intercept electrons that are being sent would cause the transmission to break. Transmission errors will result from this disturbance, which will be identifiable to authorized users (Alim et al., 2019). This is carried out to confirm the security of the supplied keys. The use of QKD requires communication between authorized users. These exchanges need to be confirmed. To do this, Numerous cryptography methods can be used. Consequently, QKD can transform an approved channel into a secure channel. One-Time Pad (OTP) encryption should be used in conjunction with QKD to provide verifiable security. In contrast, an OTP requires one-time-use keys that represent the data to be encrypted. This would significantly limit since QKD's key distribution rate is typically 10,000–10,000 times more affordable than standard optical communications. Because of this, QKD is typically used to continuously renew small encryption keys in addition to traditional symmetric encryption such as AES. To guarantee quantum-safe security, this is sufficient. Unlike existing asymmetric and symmetric cryptography techniques, quantum cryptography bases a key element of its security model not on mathematical principles but on physics ideas. This type of encryption uses natural resources and light particles to create an unbreakable cryptosystem (Rawat et al., 2023). This one maintains excellent safety precautions against riding while transmitting photons via a visual connection. The sender chooses Before photons pass through a polarizer, A single bit identification and one of four polarizations are used. 45 degrees left (zero bit), 45 degrees right (one bit), or horizontal (zero bit) in quantum cryptography (Jabber et al., 2023; Brotherton & Gupta, 2023). A single beam splitter out of two, either diagonal or vertical and horizontal that are available is employed on the receiving end to identify the polarization of each photon that is received. A photon stream is obtained at the opposite end, and the process is then repeated (Lee et al., 2020). The order in which the photon is received by the beam splitter is transmitted from the receiver to the transmitter. The polarizer sequence that was used to transmit the key is compared by the sender with this data (Nugraha & Martin, 2021). The bit sequence resulting from the removal of the photons that were read with the wrong beam splitter contains the key (Leung et al., 2020). A photon's status changes when it is read. during transmission, and the endpoints detect this change, which makes this cryptography technique incredibly powerful and impervious to hacking or eavesdropping. "Unconditional security" and sniffing detection are made possible by quantum cryptography. Cyberspace security issues for submissions like the Internet of Things and trendy towns, as well as concerns for the Internet of the future, can be resolved with the help of these elements. The title is to be written in 20 pt. Garamond font, centred and using the bold and “Small Caps” formats. There should be 24 pt. (paragraph) spacing after the last line.

3 Methodology

The current system incorporates a variety of cutting-edge models, including attribute-based encryption, Tree-based key management, multi-entry key administration, and basic client-side shared keys. The AES encryption technique serves as its foundation (Azam et al., 2022). These models have several benefits and drawbacks. For example, attribute-based encryption, or ABE, is what these models are known for. the key assignment and processing the cost of each logged-in client to the involved organization, which is the system's main drawback. Enhancing identity management through the defeat of a passive attack and side channel using multi-entry key management (Balbin et al., 2020). The main drawback is that a conflict with SLA resulted in a sniffer attack. For instance, in a 64-bit system, 4096 registers are needed to store every possible combination of ones and zeros. A qubit, on the other hand, possesses the property known as it can be both zero and one at the same time thanks to superposition. This suggests that just 64 records are needed for a 64-qubit quantum computer. More operations can be carried out simultaneously thanks to this role. Scalability also refers to the capacity to create a quantum computing system that is tiny enough to be practical in daily life. Right now, the quantum system's stability is the primary engineering challenge in quantum computing. A less efficient classical computer will arise from the quantum method If it is unstable, after superposition, it will collapse into a standard collection of ones and zeros.

- It makes too many basic algebraic concepts.
- Every data block is always encrypted in a very similar way.
- When considering both security and performance, software implementation of AES encryption in counter mode might be challenging.

Proposed Work

Establish Data security and cryptography in a distributed context are necessary to guarantee cloud data sharing in a safe environment. Therefore, this work introduces a fresh take on cryptography that provides more adaptability and a secure communication route. This service combines an improved version of the Advanced Encryption Standard (AES) with quantum key distribution (QKD) (AES). This approach also fixes important issues with distribution and administration in cloud environments: a fresh layer of cloud-based cryptography that separates current authentication and cryptography using secure gives consumers access to private keys and cloud domain accounts. It should be emphasized, though, that certain predictions claiming that all encryptions will become inoperable due to quantum computing are untrue; thus, quantum-resistant rule sets, the Advanced Encryption Standard, for example (256-bit) (AES-256), are already in existence. Quantum computing will have significant effects on cryptography in both theory and practice if it materializes and reaches its full potential. AES is one of the few algorithms that have an extra strength variation. The basic algorithm is 128 bits, with a 256-bit further power as a backup. These bits are adequate even in the case of quantum computing; however, they appear to be unavailable at least for the foreseeable future. There are several categories for computing. numerous groups according to their applications. It functions to safeguard sensitive data and customer communications, authenticating and monitoring genuine user uniqueness, offering embedded security services for a fee that customers pay, and gaining access to encryption and decryption procedures through the usage of QAES. It promises to defend against numerous malicious assaults on data contained in files accessible to distant computers. a cloud environment where QKD and CSP methods are combined. divides the data into chunks to facilitate processing. Quantum Key Distribution (QKD) uses it to detect eavesdropping and requires fewer resources to maintain. This is due to the impossibility of replicating the quantum-state-encoded data. As a result, this makes cryptography systems more efficient.

QAES Encryption Technique

The intangible plan specifies the behaviour and operation of a system. An authoritative explanation of the apparatus, the architecture, logically supports the structural attributes of a system. It provides a guide for developing products and systems that work together to execute the overall system and describes the program's building blocks. To create a secure cloud environment, data exchange between provided environments must be secured concerning data protection and encryption. Consequently, this project secures the communication environment and increases flexibility by introducing a new cryptographic service. This service makes use of both an improved edition of the Quantum key distribution (QKD) and the Advanced Encryption Standard (AES). This solution also fixes the problems associated with crucial management and distribution in cloud settings. This study presents A novel cryptographic service layer called Quantum Cryptography as a Service (QCaaS) for cloud environments. It creates a protected cloud domain and divides accounts according to the cryptographic credentials of the clients. QCaaS has several duties, one of which is to shed light on the books and websites that the dissertation's findings were derived from. Any one of these pieces or websites provides information about collective behaviour learning, including its advantages and disadvantages, current approaches, and solutions. meeting the needs of the client Concerning safe communication that protects their data, confirming and keeping an eye on the unique identity of the original user, putting in place an encryption service incorporated into every rent payment made by subscribers, as well as finishing the encryption and decryption process using QAES processes.

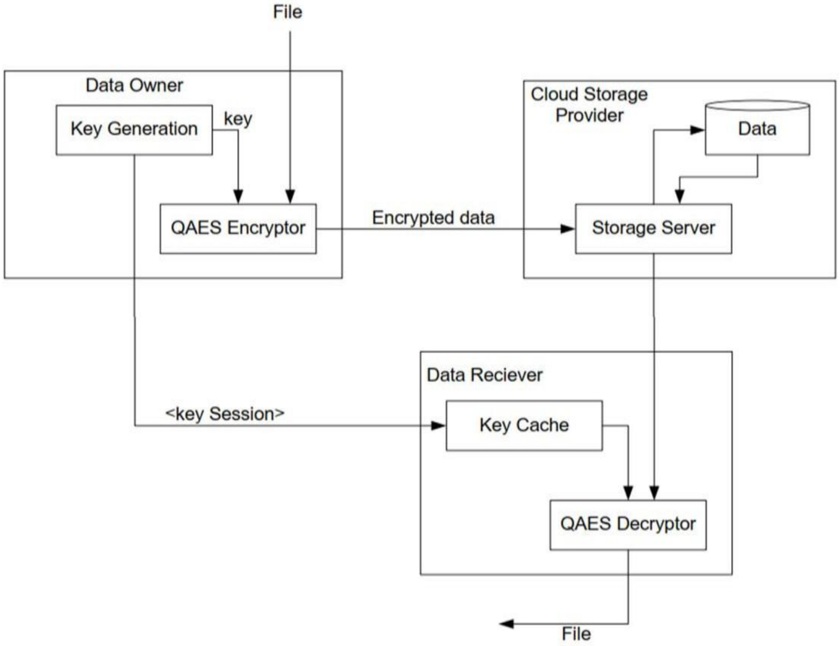

Figure 2: Cloud Data Retention Infrastructure Design

Owner of Data: This component will encrypt the file by using its key-generating capabilities. Figure 2 shows that the QAES encryption is employed here. Providers of Files are stored on the cloud using cloud storage. Data Receiver: An important meeting is sent by the data owner to the receiver. We can decode the cloud file by using this key. We employ the QAES Descriptor for decryption. One special feature of the capacity, the capacity of the two users in communication to recognize the presence of any outsider attempting to obtain the key, or any outsider seeking to intercept the key, is known as quantum key distribution. The measure is creating anomalies that can be detected.

The QAES Algorithm

Step 1: Make a set of circular keys with the cipher key.

Step 2: Designate plaintext block data as the starting value of a state array.

Step 3: The first-round key should now be included in the depending on the block size, carry out the state modification rounds.

Step 4: Continue till the very end of the manipulation by the state process.

Step 5: The final state array, or ciphertext, is copied out of the encrypted data.

By utilizing quantum superpositions, entanglement, and data transfer A communication system in quantum states that can identify eavesdroppers can be created. Like Diffie- Hellman (DH), The distribution of quantum keys is restricted to usage in producing and delivering keys; message data is not sent. The most common set of rules QKD and the one-time pad set are linked.

4 QAES Development

The QAES-developed technology offers a level of security for cipher systems based on symmetric encryption that is unrestricted. through the integration of an enhanced AES with the QKD. Figure 2 shows the QKD-generated DQS- Boxes, or dynamic quantum S-Boxes, are used in the encryption and decryption of the AES Enhanced version.

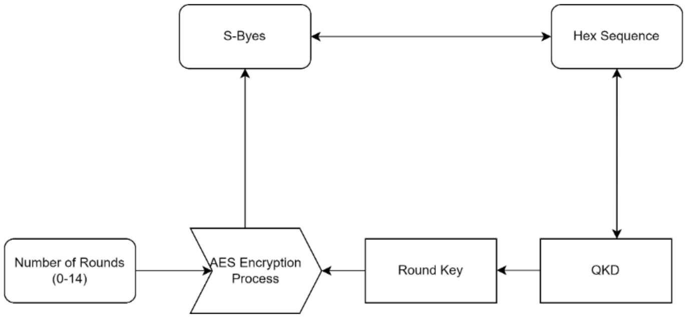

Figure 3: Configuration of QAES

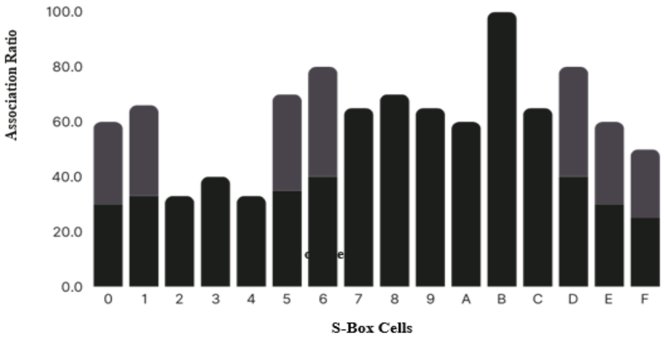

Figure 4: QS-Boxes 1 and 2 Association

The DQS boxes benefit from a dynamic method whereby each S-Box's contents alter in tandem with each round's shift in the key generation. Figure 3 shows the mechanism issues with conventional S-boxes are resolved with the use of such dynamic mechanisms. Increased resilience to attacks is ensured, and the encryption system is difficult to break since unconditional security is dependent on the Heisenberg uncertainty principle, a fundamental aspect of quantum physics, rather than a complicated Key generation founded on a model of mathematics.

- The DQS-Box is automatically produced by the method using the 256-bit secret key creation.
- Using QK1 generated by QKD round1, use the AES steps to encrypt the input file's first block (P1–128).

$$E\ (P1 \oplus qk1) = C1$$

- Lastly, use qkn, which is generated by QKD round n, to Utilize the AES steps, encrypt the final block input file.

$$E(Pn \oplus qk1) = Cn$$

- The decryption procedure begins (inverse approach) after the encrypting procedure.

$$D\ (Cn \oplus qkn) = Pn$$

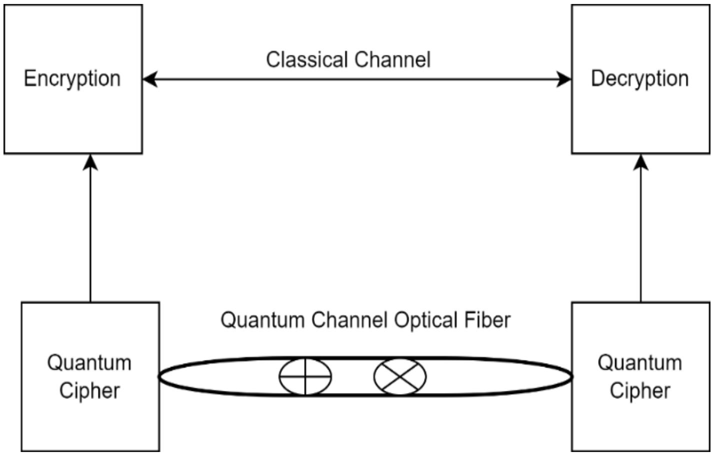

Figure 5: QAES Encryption

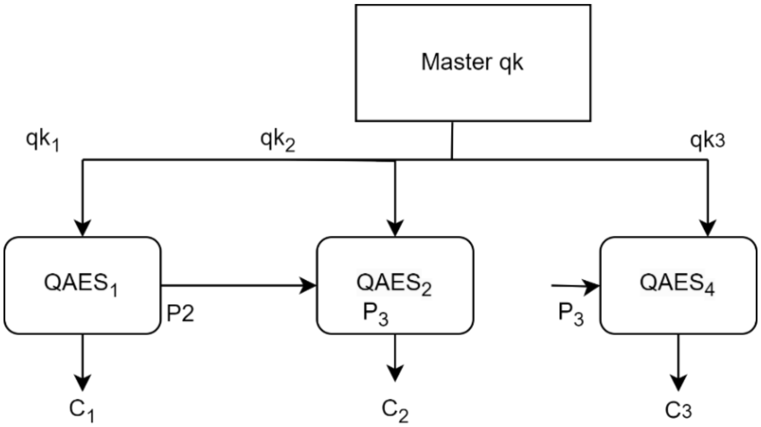

Figure 6: Encryption Process

As seen in Figures 5 and 6, The unrelated key sequence (qk1, qk2..., qkn) in each key indicates the online mode cycle. because of the QKD-related key availability (KA). The attackers are prevented from attempting to discover the next significant generation. Following that, the key sequence (qk1, qk2..., qkn) will be handled as a sequence of subkeys. for each QAES round, which is then employed in the decryption and encryption process. Lastly, this mode is compatible with all encryption modes, including the three modes: cipher counter (CTR), output feedback (OFB), and feedback (CFB).

5 QAES Performance

The QAES technique has been applied in the analysis that follows, employing multiple input file sizes: 200, 300, 500, 700, and 1000. In general, we may say that the AES is slightly faster than the QAES. For instance, the encryption time of for QAES-128 bits, the key generation time of 500 qubits is 0.07 ms, whereas the file encryption time is 0.17 ms, as shown in Figures (4–7) and Equation (1). Thus, the overall duration of QAES-128 is 0.13 ms, while QAES-192 takes 0.15 ms. Lastly, Throughout the encryption process, the input file size has consistently fluctuated, and the processed file's details stay unchanged because The AES and QAES share a similar architecture. Using the laws of quantum physics, the technique of Symmetric encryption key distribution is secured by quantum cryptography. It is more reasonable to refer to it as "quantum key distribution" (QKD). For the visual connection to work, the "quantum particles" of light, or photons, are sent there. It is clear from the tenets of quantum physics that quantum observation is a cause of confusion. Thanks to the different QKD techniques, Transmission will stop any effort to detect broadcast photons by ear. Accessible users can see the transmission failures caused by this interference. To ensure the security of dispersed keys, this is done. It takes collaboration amongst authorized users to implement QKD. It is necessary to guarantee this partnership. To do this, a variety of cryptographic methods can be applied. Consequently, QKD can use an authorized communication route to transition to a secure communication channel. By enabling users to safely exchange keys and create secure connections that can be opened by hearing offensive speech; to transmit secure connections, quantum key distribution (QKD) makes use of concepts from quantum physics. While QKD secures quantum certificates, Heisenberg's uncertainty, which states that Random One of the two divided quantum segments that produce photons measuring a photon's quantum area requires changing the quantum information itself, is the foundation upon which the crucial exchange operates. If the portals are not altered, the two linked contacts can therefore verify that they are safe to use and have a shared private key. The quantum substance of the photons is altered when a malevolent entity tries to obtain crucial information by reading or blocking a message. Stakeholders are alerted to the hazard and should not trust the communication when even a single photon picture is observed. Theoretically, one-time pad (OTP) encryption and QKD must work together to provide attainable security. If the data is to be encrypted, OTP requires long keys that are only used just once. This will rigorously limit QKD key distribution because it is often ten thousand to one million times lower than that of traditional visual communication. the amount of bandwidth that may be used.

6 Results and Discussions

Which are applied to the conventional S-boxes correlation and independence calculations in Equation, are primarily responsible for the independent ratio. As a result, the DQS- Box-based ratio of independence is computed. According to the findings, applying the DQS-Box resulted in a larger ratio and a lower correlation coefficient. amid various rounds. This ensures increased security, resistance to nearly all cryptanalysis assaults, and the development of a more robust encryptionscheme.

$$\text{ratio max standard CORR } x = (1)$$

Where the correlation ratio is denoted by CORR. As an illustration, two DQS-Boxes of 256 bits (matrix 16 × 16) are constructed concerning the QKD simulation environment. Between QS-Box1 and DQS-Box2, the ratio of independence and correlation functions is shown. The ratio of dependence is 97.67%, and the coefficient of correlation ratio (CORR) is 7.752%. To be precise, for every corresponding row between two QS-Boxes, the proportion of autonomous ranges between (83.56% - 100%). Additionally, the intermediate generation used in the process of decrypting and encrypting benefits the DQS-Box generation process attack linked to the S-Box. The QAES algorithm has been applied to the following analysis utilizing a range of input file sizes: 200 kb, 300 kb, 500 kb, 700 kb, and 1000 kb. The implemented algorithms' running times employing the above-discussed local machines are shown in Figures 7 and 8. Kilobytes are used to measure the input size, and the running times are calculated in milliseconds (ms). Higher security is seen when comparing the QAES encryption algorithm to the conventional AES encryption algorithms.

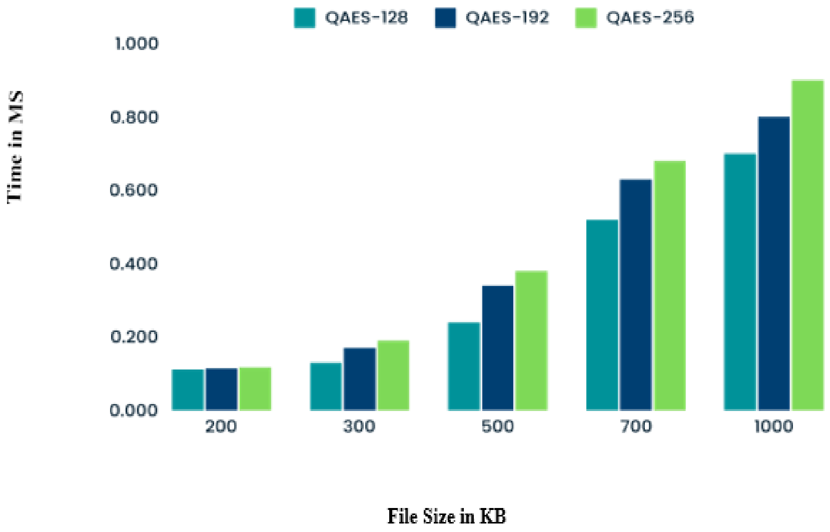

Figure 7: Performance of QAES

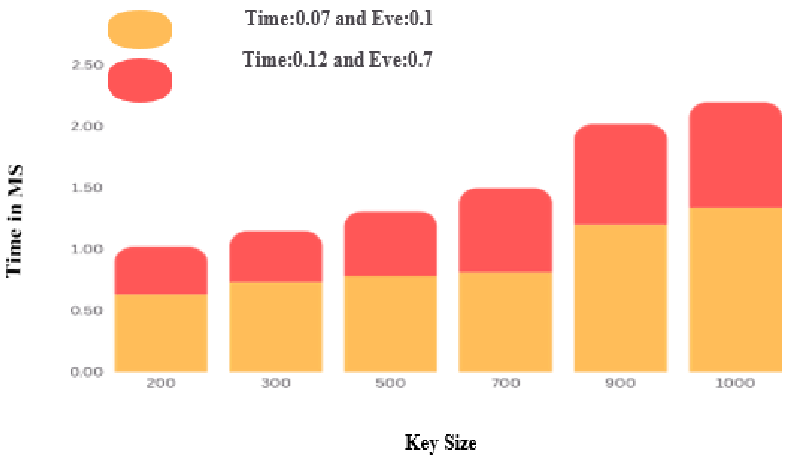

Figure 8: Unique Settings for Secret Key Management

Data User: Consists of two blocks, an offline keyword file, and an audio port. To request files encrypted by the cloud, utilize the offline key file and the audio port to establish a link. Three fields are included in the data owner: listen port, user port, and user IP. The shared device's IP address can be found using the IP address of the user. The port for listening and the user port can be used to determine the user's port address used to connect via the cloud. Cloud: The infrastructure that allows us to browse and transfer files to the cloud after the encryption using QAES algorithms upload the contents to the cloud.

The user demands cloud- based encrypted files. Because of cloud computing, users can access documents via the Internet, run software without needing to install it, and ensure a safe setting for the customer and the CSP. However, this rapid growth in cloud computing presents additional challenges for the extremely important security management function. This study offers a solid remedy for complex cloud security problems. environments with QCaaS. Most attempts generally outperform others in some way, particularly in terms of producing the private keys needed for encryption and decoding. This can view such a leading cloud component to integrate the cloud based QKD and CSP ideas approach.

7 Conclusion and Future Works

The swift growth in cloud computing usage has made security management's job, which is essentially more challenging responsible for establishing a safe environment for the CSP and the client. A solid remedy for the escalating security problems in cloud systems is offered by this study. Maintain critical data security and offer customers secure communications. Keep an eye on and confirm that the unique operator is unique. offering cloud-based encoding services that consumers can rent; and to carry out the encryption and decryption procedure, use QAES. All things considered, our efforts outperform those of our rivals in several ways, particularly in terms of producing private keys that are necessary for decryption as well as encryption. This is thought to be the original cloud environment. to incorporate the CSP principle in addition to the QKD approach. A Third Trust Party (TTP) will eventually need to be added to connect your cloud environment to your customer. TTP serves as a crucial cryptography cloud for key creation and creates a trustworthy environment between the two parties. Quantum computing is superior to traditional computing. Before its practical application, quantum computing requires extensive research and development. There are certain disadvantages to quantum cryptography despite the increased security. One of the main restrictions on the security that quantum cryptography may offer. The spectrum of quantum cryptography's capabilities is constrained by interference. This means that as the distance from an object grows, so does the probability of a photon impacting or colliding with other objects. To avoid being intercepted, a single photon is sent throughout each time interval. This work presents, implements, and discusses an evolved QAES is the abbreviation for the AES algorithm, which is based on dynamic S-Boxes and quantum encryption mechanisms. The study demonstrates that, since all mathematical requirements are met, the construction and design of QAES do not conflict with the security of the AES algorithm. The research and experimental findings demonstrate that, in comparison to the AES-generated keys, the QAES generates more complex, unbreakable keys that are difficult for adversaries to predict. The QAES power comes from its capacity to provide a high degree of DQS-Box independence. Algebraic and quantum attacks will be used in the future to ensure the QAES strength and the outcomes will be examined thereafter.

References

[1] Albert Carlson, Q. S. A., Sharkey, K. L., QSME, Q., Watchorn, M. S., QIS, Q., & Mumm, H. C. (2022). NIST Quantum Proof Algorithm Analysis.

[2] Alim, A., Zhao, X., Cho, J. H., & Chen, F. (2019). Uncertainty-aware opinion inference under adversarial attacks. *In IEEE International Conference on Big Data (Big Data)*, 6-15.

[3] Azam, M., Ali Khan, M. S., & Yang, S. (2022). A Decision-Making Approach for the Evaluation of Information Security Management under Complex Intuitionistic Fuzzy Set Environment. *Journal of Mathematics*, *2022*(1), 9704466. https://doi.org/10.1155/2022/9704466

[4] Balbin, P. P. F., Barker, J. C., Leung, C. K., Tran, M., Wall, R. P., & Cuzzocrea, A. (2020). Predictive analytics on open big data for supporting smart transportation services. *Procedia*

Computer Science, *176*, 3009-3018.

[5] Brotherton, M., & Gupta, M. (2023). A Survey of Quantum Computing for Cloud Security. *In Future Connected Technologies*, 1-34.

[6] Harnoš, P., & Dedera, Ľ. (2021). Analysis of current trends in the development of DSLs and the possibility of using them in the field of information security. *Science & Military Journal*, *16*(2), 15-27.

[7] Jabber, S. A., Hashem, S., & Jafer, S. (2023). Secure Cloud Computing by A dual-Layer Encryption Mechanism. *Preprints.* https://doi.org/10.20944/preprints202312.0615.v1

[8] Kholod, I., Shorov, A., & Gorlatch, S. (2020). Efficient Distribution and Processing of Data for Parallelizing Data Mining in Mobile Clouds. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *11*(1), 2-17.

[9] Korać, D., Damjanović, B., & Simić, D. (2022). A model of digital identity for better information security in e-learning systems. *The Journal of Supercomputing*, 1-30.

[10] Lee, H. J., Cho, S. H., Seong, J. W., Lee, S., & Lee, W. (2020). De-identification and privacy issues on bigdata transformation. *In IEEE International Conference on Big Data and Smart Computing (BigComp)*, 514-519.

[11] Leung, C. K., Elias, J. D., Minuk, S. M., De Jesus, A. R. R., & Cuzzocrea, A. (2020). An innovative fuzzy logic-based machine learning algorithm for supporting predictive analytics on big transportation data. *In IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, 1-8.

[12] Malathi, K. (2024). Improved Dynamic Regression Framework for Effective Data Management in Wireless Networks on Cloud-assisted Internet of Everything Platform. *Journal of Internet Services and Information Security*, *14*(2), 169-188.

[13] Neelima, S., Manoj, G., Subramani, K., Ahmed, A., & Mohan, C. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. *Indian Journal of Information Sources and Services*, *14*(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21

[14] Nugraha, Y., & Martin, A. (2021). Towards a framework for trustworthy data security level agreement in cloud procurement. *Computers & Security*, *106*, 102266. https://doi.org/10.1016/j.cose.2021.102266

[15] Ouda, A. J., Yousif, A. N., Hasan, A. S., Ibrahim, H. M., & Shyaa, M. A. (2022). The impact of cloud computing on network security and the risk for organization behaviors. *Webology*, *19*(1), 195-206.

[16] Rawat, R., Chakrawarti, R. K., Sarangi, S. K., Patel, J., Bhardwaj, V., Rawat, A., & Rawat, H. (Eds.). (2023). *Quantum Computing in Cybersecurity*. John Wiley & Sons.

[17] Shiraishi, Y., Mohri, M., & Fukuta, Y. (2011). A Server-Aided Computation Protocol Revisited for Confidentiality of Cloud Service. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2*(2), 83-94.

[18] Sonya, A., & Kavitha, G. (2022). A Data Integrity and Security Approach for Health Care Data in Cloud Environment. *Journal of Internet Services and Information Security*, *12*(4), 246-256.

[19] Sriram, G. S. (2022). Resolving security and data concerns in cloud computing by utilizing a decentralized cloud computing option. *International Research Journal of Modernization in Engineering Technology and Science*, *4*(1), 1269-1273.

[20] Tukkoji, C. (2024). Secure Data Storage in Cloud Computing Using Code Based McEliece and NTRU Cryptosystems. *SN Computer Science*, *5*(4), 1-14.

Authors Biography

E. Geetha Rani, (Member IEEE) is working as Assistant Professor in the Department of Computer Science and Engineering, Alliance University, Chandapura, Anekal, Bengaluru, Karnataka. Received Bachelor degree in Information Technology from Koneru Lakshmaiah College of Engineering. Master degree in Computer Science and Engineering from Acharya Nagarjuna University and Pursuing Ph.D in Computer Science and Engineering from GITAM University. Acting as Editor, Board Member and Reviewer for Various Journals and Conferences. Has 12 years of experience in Teaching and Research and Industry. Having IEEE and SCRS membership and publishing various Journals and Conferences papers indexed in Scopus. Area of research includes Data Analytics, Cloud Computing, Soft Computing, Image Analysis, Security Issues, Communication Network and Deep Learning, Social Media Analytics.

Dr. Chetana D. Tukkoji, is a distinguished researcher and educator in the field of Computer Science and Engineering, with a notable portfolio of publications and academic contributions. Her work spans various national and international conferences and journals, showcasing a keen interest in emerging technologies and their applications. Dr. Chetana research primarily focuses on Cloud Computing, Big Data Analytics, and Machine Learning. She has published more than 30 publications in national/international journals. Undertook numerous FDPs and workshops focusing on advanced topics such as Deep Learning, Cyber Security, and Machine Learning. Published two patent applications. She has completed certification courses in Data Science with R Programming, Robotic Process Automation, Python, and Salesforce Developer platform with demonstrating continuous professional development.