International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Operative Encryption Method with Optimized Genetical method for Assuring Information Security in Cloud Computing

Ved Prakash Mishra[1], Dr V S Krushnasamy[2], Faiz Akram[3], Hendy Tannady[4], Nishant Kumar Pathak[5]

Submitted: 24/04/2023 **Revised**: 14/06/2023 **Accepted**: 26/06/2023

Abstract: The cloud customer is typically uninformed of the provider's threat assessment and mitigation procedures. Ask what safety precautions the service provider takes. So, the client must likewise do something to improve the supplier's security. The function of quantum key distribution (QKD) in cryptographic infrastructures is investigated in this work. QKD uses quantum mechanical systems to promise safe key agreements. There is a claim that QKD will play a significant role in upcoming cryptographic infrastructures. Without relying on computational assumptions, it can guarantee long-term confidentiality for encrypted data. In fact, even when using public-key authentication, we contend that QKD still provides stronger security than conventional key agreements. Several researchers have put forth various data recovery strategies, but they are ineffective and unreliable. When the primary cloud server loses its data and is unable to offer data to users, the proposed technique gives the user the option to acquire information from any backup server in order to achieve reliability. The decryption procedure is then carried out in response to the user's request. Experiments were done to demonstrate the applicability of the proposed frameworks, and performance indicators were compared to those utilized by other researchers. Based on this study, a framework is developed, that guarantees authentication and lays the way for safe data access, with better performance and fewer complications than the previous efforts.

***Keywords*:** *Encrypted Data; QKD, OGA, Throughput.*

1. Introduction

Typically, the cloud consumer is unaware of how the provider assesses and handles threats. And what security measures the provider employs. To increase the security provided by the supplier, the client needs thus also take some action. Better than relying solely on the standards set by the provider to manage data security. It's a good idea for the consumer to encrypt the data before delivering it to the supplier [1].

After sending data to the cloud, the client no longer has control over it; instead, the cloud provider is in charge of it. As a result, encryption is crucial for maintaining the confidentiality of data. Depending on the Cloud service models, there are numerous approaches that can be used to accomplish the difficult task of cloud encryption [2]. Since the customer has the least influence over the infrastructure with SaaS, there are fewer dangers, whereas, with IaaS, the customer has greater control and is in charge of the security measures. The usefulness of encryption in the Cloud service models is examined in this section [3].

Following receipt of the data from the client, the cloud provider encrypts it. This would safeguard data confidentiality from outside threats and allow the provider to retransmit or store the data in an encrypted form. Secure SSL/TLS channels are used between the client and the provider to transmit data from the consumer to the latter. Yet, it raises extra security concerns to let the same source handle both the data encryption and the data storage [4]. Prior to transmitting the data to the cloud, the customer might encrypt it using an encryption method unrelated to the provider. When the client accesses the data, it has been decrypted after being transmitted to the supplier. In this instance, the encryption algorithm and the keys are entirely under the customer's hands [5]. Given that the provider lacks the decryption key, the SaaS application can only perform a restricted number of activities on the encrypted data (such as searching). The SaaS application

1Associate Professor, Computer Science and Engineering Amity University Dubai , Uae
mishra.ved@gmail.com
orchid id: 0000-0003-1832-8736"
2Associate Professor, Department of EIE Dayananda Sagar College of Engineering
krushnasamy-inmt@dayanandasagar.edu
0000-0001-7529-3782
3Assistant Professor, Faculty of Computing and Informatics, Jimma Institute of Technology, Jimma University, Jimma, Ethiopia
akram.faiz@ju.edu.et
4Department of Management Universitas Multimedia Nusantara, Banten,
Indonesia
hendy.tannady@umn.ac.id
https://orcid.org/0000-0001-6911-7010
5Asst. Professor, Department of Computer Science Shobhit Institute of Engineering & Technology (Deemed to-be University)
nishant.pathak@shobhituniversity.ac.in
ORCID: 0000-0002-2841-4550

could occasionally be unable to read or recognize the encrypted data. For instance, the message won't reach the recipients if the email sender encrypts it before sending it to the email provider (SaaS provider). Without the decryption key, the email provider is unable to decipher the message and determine the recipient's email address [6].

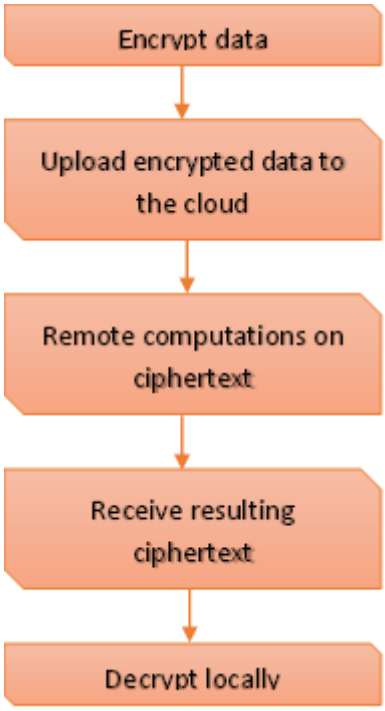

Fig I: Cloud cryptography Sequence.

Quantum cryptography, and in particular Quantum Key Distribution (QKD), has attracted considerable technical and public interest since its discovery [7]. The discussion in this work is limited to quantum cryptography and quantum key distribution (QKD). However, almost all of these need a medium- to large-scale quantum computer to be implemented [8].

A lot of data can be saved in a cloud environment. Services for data recovery are required to keep that data functioning properly. Large amounts of personal data are stored on the primary cloud in cloud computing. As a result, the demand for recovery services is increasing daily, necessitating the creation of a strategy for efficient and successful data recovery services. The recovery technique's goal is to assist the user in gathering data from any backup server in the event that the primary server is unable to do so [9]. Data on the cloud can be recovered via a variety of processes, including the backup strategies. However, there are some drawbacks to those methods, including implementation difficulties, security concerns, and lengthy retrieval times. These are the key problems with the current system. In our suggested system, we use an efficient genetic algorithm for data recovery to fix these problems [10].

When it comes to restoring lost data from backup copies, there is a growing demand among organizations for dependable processes that are not only low-cost but also place a minimal amount of strain on the organization. As a result of advancements in applications and the availability of a variety of devices, there is a pressing requirement for the development of backup strategies that are capable of ensuring a higher level of data integrity, of simultaneously managing a large number of devices, and of successfully restoring data [11]. The failure of an enterprise to carry out a backup operation as planned may have a significant negative effect on the business's finances. This is because the expense of replacing lost data, the possibility of delays and legal action, as well as lower productivity, all contribute to the likelihood of adverse monetary outcomes. Because of this, the company can end up going out of business gradually over time. When used by businesses to back up their data, cloud storage can improve its properties such as being cheap and cost-effective when compared to more conventional techniques such as discs and tapes, where managing and transporting the media can be difficult [12]. Cloud storage can also improve the properties of the data being backed up, such as the data's ability to be easily accessible.

2. Past Related Work Done

Initially, the Privacy and Utility (PU) coefficient was calculated using the PUBAT algorithm. Next, using the PU coefficient and the data used as input for data posting, the privacy-preserved data were identified. The technique tested three different datasets for the accuracy and database difference ratio (DBDR) evaluation measures

[13]. This strategy outperformed all other methods in terms of DBDR and accuracy, demonstrating its effectiveness. The performance had to be enhanced, which was a drawback of this approach. A few scientists developed a method that helped Content-Based Image Retrieval (CBIR) on encrypted photographs that were free of sensitive data stored on cloud servers. The feature vectors were initially extracted from the photos and used to represent them [14]. Then, by building the pre-filter tables with locality-sensitive hashing, the search efficiency was improved. Finally, the feature vectors were secured using the k-Nearest Neighbor (kNN) technique. The experimentation and security analysis proved the effectiveness and security of this strategy. This method's disadvantage is that it necessitated additional security enhancements. The features in the encrypted photographs were to be extracted as a future improvement to this technique [15].

Researchers created a remote data possession checking the system for cloud storage that uses privacy-preserving authenticators. In this case, the cloud service provider and public verifier were unable to access the actual authenticators [16]. This technique was used when contracts and electronic checks were successful to verify the accuracy of cloud data. The Homomorphic Invisible Authenticator (HIA) was created in this situation to protect the authenticator's privacy and to assist in blockless verification. The remote data possession checking strategy was then created based on the HIA. The effectiveness and security of this strategy were examined using simulation and theoretical studies. The outcomes of the experimentation demonstrated how effective and secure this strategy was [17].

Depending on the user's position, a group of employees provided a privacy-preserving Data Sharing Scheme (DASS) to methodically ensure the security demands of the users for social apps. A multi-user searchable encryption strategy, a dynamic social attribute management model, and a fine-grained access control approach were the three methodologies used in this scheme [18]. This scheme produced an associated access control message for the data owner dependent on the attribute group key management mechanism and the CP-ABE, allowing the data owner to describe the access control strategy and impose the data owner's files. The data owner achieved resilience to collusion attacks, rapid attribute revocation, and fine-grained access control by securely and widely disseminating the data [19]. The authors provided details of a search control message and an assigned trapdoor message to aid in efficient attribute revocation and search facilitation in dynamic social membership. The findings of the performance evaluation demonstrated the effectiveness, fine graininess, and security of this plan [20].

Some academics examined the existing privacy protection strategies and presented privacy protection approaches based on ranked multi-keyword searches and probabilistic public-key encryption. The file collection was first given an index, and both the index and the file collection were afterward encrypted and stored on the cloud. In order to extract the data files, the authorized user created the trapdoor and sent it to the cloud server [21]. The server began a file search on the encrypted data through the trapdoor and gave the user any matching files. This method's probabilistic public-key encryption improved efficiency. The process verified the accuracy of the data. To illustrate the effectiveness of this method, performance, and security analyses were conducted. The analysis findings indicated that this method was effective and highly secure. However, the strategy necessitates dynamic data processing and ranked keyword searches on encrypted big data on the cloud [22-23].

The method was used to remove the high-impact data blocks from the nodes that were in danger of going out of business. Then, the user rank reference was used to optimize the cloud storage system [24]. The authors also presented the data leakage model, which distinguished between single-point and multiple-point settings for data leakage. Indirect leakage and direct leakage were the two different types of data leakage. The simulation was used to examine how well the strategy worked, and the results showed that it significantly reduced the amount of private data that leaked into either a public or private cloud [25].

3. The Objective of the Work

1) To research the authentication, privacy-preserving, data recovery, and classical cryptography techniques used in cloud computing.
2) To develop a framework to address all those security issues with minimal computational overheads, ensuring secure data storage and access to the various cloud resources and implementing it.

4. The Projected Work:

In this paper, we analyse how Quantum Key Distribution (QKD) functions in secure networks. QKD uses quantum mechanical systems to guarantee safe key agreement. In this paper, we believe that quantum key distribution (QKD) will play a significant role in the development of future cryptographic infrastructures. Without relying on computational assumptions, it can ensure the permanent secrecy of encrypted data. We claim that QKD still provides superior security over classical key agreement, even when utilizing public-key authentication.

When compared to traditional cryptography, QKD is a novel tool since it enables secure key agreement where the output key is completely independent of any input value.

QKD can be used to construct systems with new security features, but it does not replace the necessity for other cryptographic primitives like authentication. In quantum key distribution (QKD), Alice and Bob each obtain and measure some quantum state. To decide which of their measurement findings could yield secret key bits, they confer (from this point on, all communication is classical) and sift out those for which the measurement parameters were incompatible. After correcting for errors, they calculate a security parameter that describes how much of a secret could be leaked to an eavesdropper. When this number rises above a certain point, they call it quits because they are unable to provide complete confidentiality. If it is less than the threshold, then privacy amplification can be used to eliminate the eavesdropper's ability to deduce any additional information and arrive at a common secret key. To prevent man-in-the-middle attacks, some of this traditional communication must be verified. There is a small chance that the protocol will fail at some point.

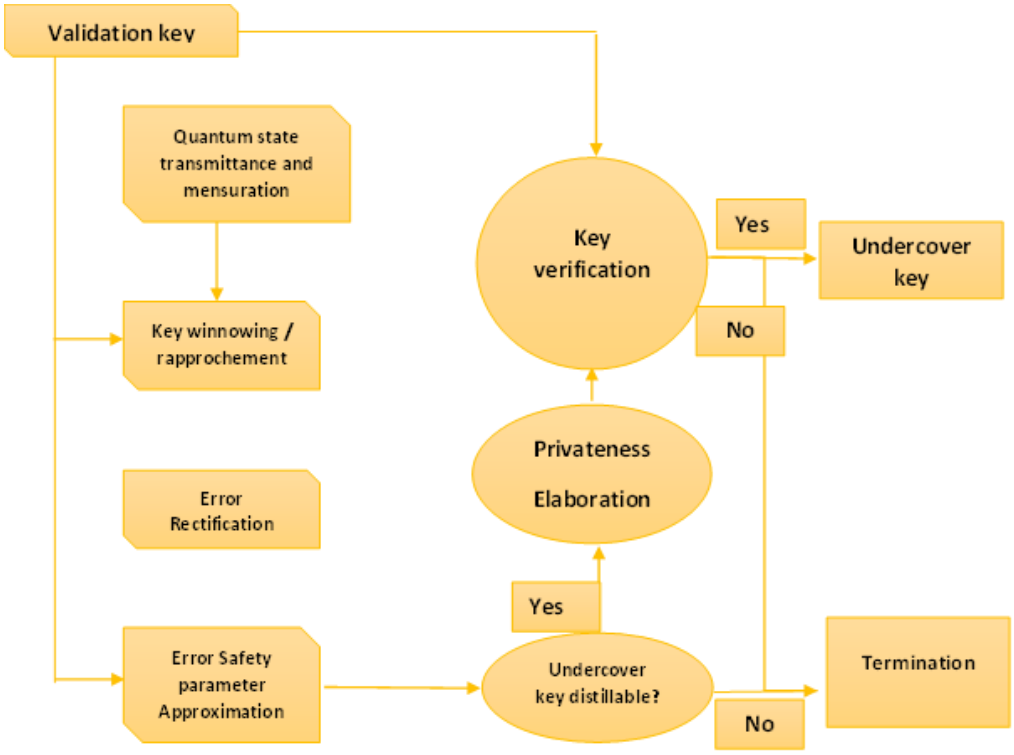

Fig II: Phase of quantum key distribution Algorithm.

In Figure II, we see a flowchart outlining the steps involved in distributing quantum keys. Once a secret key has been generated via QKD, it can be put to many different uses. Using it as the secret key in a one-time pad is the most frequent method for achieving unbreakable encryption. Subsequent QKD rounds can employ classical authentication with the key. As work on QKD progresses, we can anticipate QKD devices that are more secure, less complicated to set up, cheaper, and more compact, possibly even being able to fit on a single circuit board.

When compared to cyphers employed without QKD, the security provided by hybrid QKD systems is superior. To improve forward secrecy in the face of key compromise, the QKD subsystem frequently supplies new, independent keying material that can rekey the classical block or stream cypher. This reduces the risk of attacks against the underlying cypher that use many plain texts or cipher texts encrypted under the same key.

In the next part, a comprehensive method breakdown of the suggested model will be shown.

- The First and Subsequent Steps: This is accomplished by establishing a quantum link between the owner's data and the QKDS in order to swap a quantum key for use in the subsequent iteration of our suggested model. This is done in order to protect the data of the owner.
- Third step: use the QKDS database() function to permanently store the key and then retrieve it as needed. The QKDS and the owner data have come to an agreement on a unique identifier for the database. This identifier is represented by the first ten bits of a basis that is generated at random and given to the owner data. Both parties believe that this identifier is the only one of its kind.
- In the fourth and fifth steps, we combined the DH encryption technique with two other algorithms because there are many ways to encrypt data and we wanted to maximize the effectiveness of each.
- The goal of the uploading procedure is to transfer the encrypted information to the cloud. Aneka cloud is

more popular than other clouds, hence we should use it for our projects. APIs may be accessed quickly and easily with the help of zen server, a software toolset for digital transformation.

- In order to grant the key, which is accomplished through an authenticated classical channel, Step 7 and Step 8 require the user to obtain ID from the owner's data (that can be done through any secure way).
- Users can start exchanging keys in Step 9 after they have the ID necessary to connect to the QKDS in Step 10. To kick off the procedure, first authentications are necessary. Furthermore, some information are saved in the database using to compare with the user's ID to authenticate the procedure, adding an extra layer of security and guaranteeing the key is discovered in our database. If the key is present in the database, the process will continue to the next phase.
- After Step 11 has been finished and the key has been verified as being present in our database, Step 12 initiates the QKDS initiating the quantum connection to exchange the key with the user. To establish a quantum link, the EBB84 protocol is used to produce and transmit a random key.
- After obtaining the key from QKDS, the user can retrieve the encrypted data from the cloud and begin the decryption process to obtain the original data for his purposes (Step 13).

In the suggested system, we use the QKD encryption technique to create the encryption so strong that it cannot be broken or decrypted by an attacker or a cloud provider's service. We used the hybrid encryption methods to make sure the data we transferred to the cloud was secure, despite the fact that their processing time was the highest of the existing algorithms we considered.

Time spent encrypting and decrypting data, as well as throughput, bit error rate, and network mode analysis, are measured to demonstrate the effectiveness of the suggested approach.

5.1. Encryption Time:

Within a fixed window of time, the encryption algorithm transforms the plain text into the cipher text. Encrypting data using the planned framework and an improved application of the Genetic Algorithm technique for encryption adds time to the process. The encryption time is denoted by the, where C is the encryption computation time and R is the encryption response time. It's how long it takes from when a request is made to answers start coming back.

$$\text{Encryption Time} = \frac{C}{R} \quad (1)$$

5.2. Decryption Time:

To decrypt a message, an algorithm must take the cipher text and transform it into plain text within a certain amount of time, called the decryption time. After being decrypted via the planned framework, the data can be accessed in a shorter amount of time. Where, D is the decryption computation time and S is the decryption response time.

$$\text{Decryption Time} = \frac{D}{S} \quad (2)$$

New Quantum Key Distribution using Non-Commutative Encryption Framework is compared to other approaches in terms of how long it takes to encrypt and decode data using each. Table I below displays the outcomes of these comparisons.

5.3. Success rate is defined as follows:

Success Rate = (Number of Success attempts + External failure / Total number of attempts*100) (3)

5.4. Faliure rate is defined as follows:

Failure Rate = Dissension the failures count by the whole number of Time (4)

5. Result and Discussion:

Table 1: Evaluation Parameter Comparison of Proposed Method with Exiting Approach.

S. No.	Evaluation Parameter	Existing Method [12]	Proposed Method
1	Encryption Time (ms)	549	310
2	Decryption Time (ms)	518	306
3	Success Rate	100	98
4	Faliure Rate	65	96

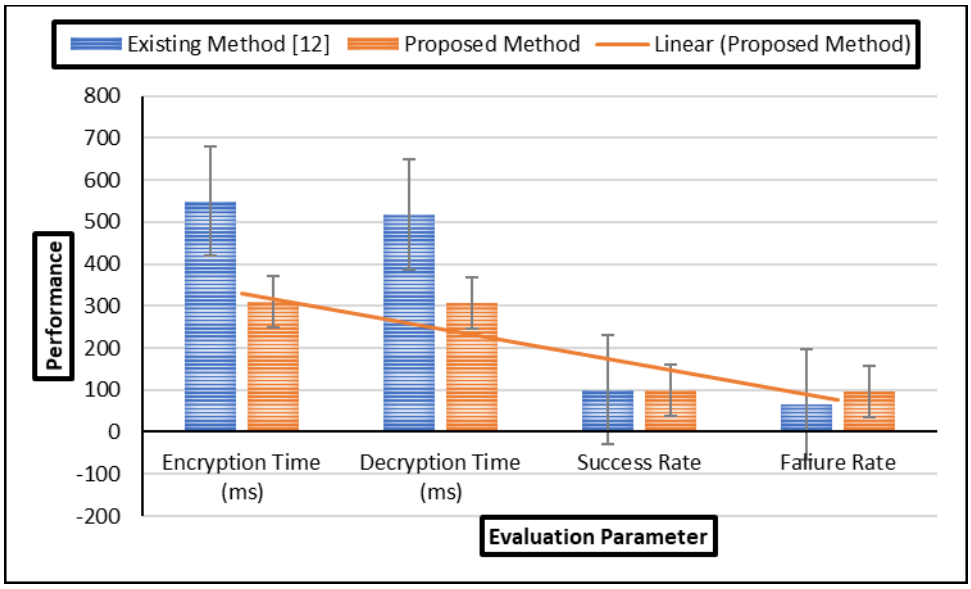

Fig III: Evaluation Parameter Comparison of Proposed Method with Exiting Approach.

Public cloud deployments have a 96% failure rate, as seen in Figure III. There is a 98% chance of obtaining efficient main distribution. We also found that the "Quantum in Cloud" platform's key generation using QKD devices was one hundred percent effective with a 65 percent failure rate in our testing. The results and comparisons presented above demonstrate that the suggested framework is more efficient at delivering data security with less investment of computational resources.

5.5. Throughput = sum ((successful packets count)*(mean packet size))/ Whole time sent in delivering that measure of information. (5)

5.6. Because of the avalanche effect, even a slight modification to the plain text (or the key) should result in a substantial alteration to the cipher text.

$$\text{Avalanche Effect} = \frac{\text{Bit count changed in cipher text}}{\text{Bit count changed in cipher text}} \quad (6)$$

Table II: Throughput examination of projected and existing method with various file sizes

S.No.	File Size	Existing Method [12]		Proposed Method	
		Throughput	Avalnche Effect	Throughput	Avalnche Effect
1	100	0.728	62.45	0.849	64.28
2	200	0.416	62.27	0.528	64.19
3	300	0.281	62.38	0.317	64.79
4	400	0.183	62.19	0.151	64.26
5	500	0.159	62.47	0.127	64.37

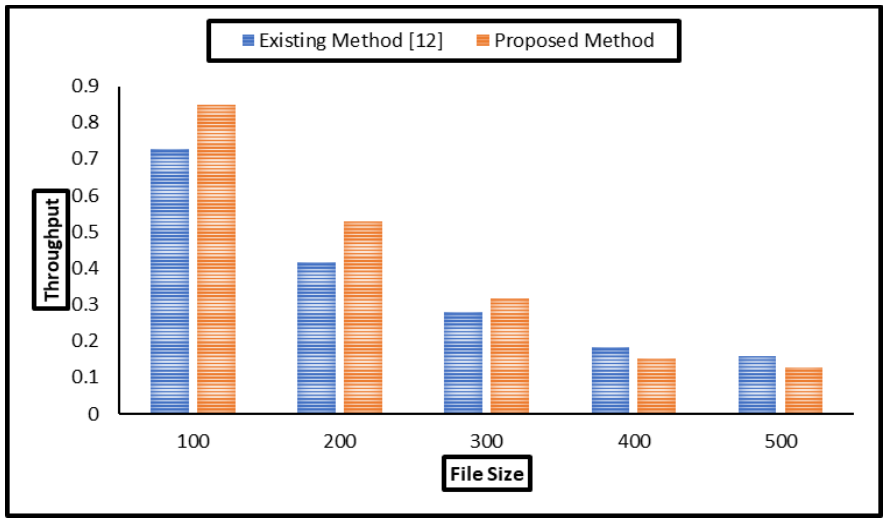

Fig IV: Thorughput Comparison of proposed method with existing approach.

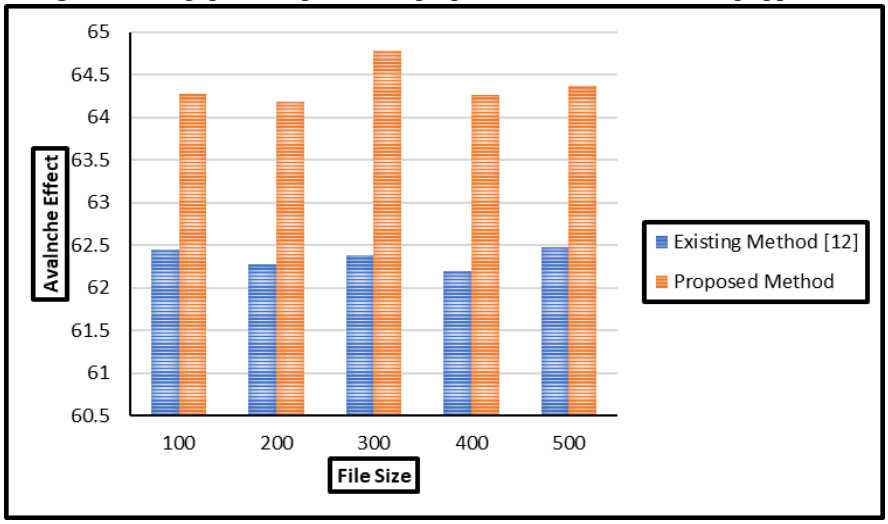

Fig V: Avalanche Effect Comparison of proposed method with existing approach.

Table II compares the current methods' throughput and Avalanche impact values to those of the proposed method. Figure IV below illustrates how this is calculated. We test a variety of encryption methods on a range of file sizes. Based on these findings, we conclude that our suggested approach offers a maximum average throughput of 0.8449, which is superior to the state-of-the-art. Figure V below illustrates how this is calculated. This demonstrates that with just a single bit of variation in the key value, our proposed method can produce an effective avalanche value. It safeguards our proposed method on the Aneka cloud infrastructure.

6. Conclusion:

Instead of storing and processing data on a single server in a single location, cloud computing distributes these tasks across a network of remote servers accessible via a central online service. In the past few years, cloud computing has rapidly advanced from a nice-to-have to a necessary component of many modern web-based endeavors. Finding a solution to successful cloud planning is one of the primary challenges in the cloud. While data processing on the cloud is likely to be secure, the same cannot be said for data transit. Over and beyond the standard 512-bit key size, we have implemented this architecture in the Aneka cloud with the addition of secure key transmission and data backup services. In this paper, we offer a unique method of Quantum Key Distribution that makes use of a non-commutative encryption scheme. In addition, OGA has been used in our proposed study for safe data retrieval. Our suggested approach significantly mitigates potential security breaches, allowing for safe data storage and transmission at a lower computational cost. The suggested framework is compared to existing methods to demonstrate the work's superiority.

Conflict of Interests:

The authors declare that there is no conflict of interests regarding the publication of this paper.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Chandramohan Dhasarathan, Vengattaraman Thirumal & Dhavachelvan Ponnurangam 2017, _A secure data privacy preservation for on-demand cloud service,‘ Journal of King Saud University - Engineering Sciences, vol. 29, no. 2, pp. 144-150.

[2] Chandramohan, D, Vengattaraman, T, Rajaguru, D & Dhavachelvan, P 2016, _A new privacy preserving technique for cloud service user endorsement using multi-agents,‘ Journal of King Saud University - Computer and Information Sciences, vol. 28, no. 1, pp. 37-54.

[3] Chang Guo, QingniShen, Yahui Yang & Zhonghai Wu 2015, _User Rank: A User Influence-Based Data Distribution Optimization Method for Privacy Protection in Cloud Storage System,‘ In Proceedings of the IEEE 39th Annual conference on Computer Software and Applications Conference, pp. 104-109.

[4] Changhee Hahn & JunbeomHur 2016, _Efficient and privacy-preserving biometric identification in cloud,‘ ICT Express, vol. 2, no. 3, pp. 135-139.

[5] Chen Lyu, Shi-Feng Sun, Yuanyuan Zhang, AmitPande, Haining Lu & DawuGu 2016, _Privacy-Preserving Data Sharing Scheme over Cloud for Social Applications,‘ Journal of Network and Computer Applications, vol. 74, pp. 44-55.

[6] Chintureena Thingom 2014, _A Study on Tools for Cloud Disaster Management‘, International Journal of Interdisciplinary and Multidisciplinary Studies.

[7] Stergiou, C., & Psannis, K. E. (2017). Recent advances delivered by Mobile Cloud Computing & Internet of Things for Big Data applications: a survey. International Journal of Network Management, 27(3), e1930.

[8] Aceto, G., Persico, V., & Pescapé, A. (2020). Industry 4.0 & health: Internet of things, big data, & cloud computing for healthcare 4.0. Journal of Industrial Information Integration, 18, 100129.

[9] Khayyat, M., Elgendy, I. A., Muthanna, A., Alshahrani, A. S., Alharbi, S., & Koucheryavy, A. (2020). Advanced deep-learning-based computational offloading for multilevel vehicular edge-cloud computing networks. IEEE Access, 8, 137052-137062.

[10] Alam, T. (2020). Cloud Computing & its role in Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), 108-115.

[11] Drake, J. H., Kheiri, A., Özcan, E., & Burke, E. K. (2020). Recent advances in selection hyper-heuristics. European Journal of Operational Research, 285(2), 405-428.

[12] S. E. Alaojan and A. H. Alwattar, "A Modified Blowfish Algorithm to Secure Data in Cloud," 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2022, pp. 218-222, doi: 10.1109/ISMSIT56059.2022.9932817.

[13] Wei, H., Bao, H., & Ruan, X. (2020). Genetic algorithm-driven discovery of unexpected ther-mal conductivity enhancement by the disorder. Nano Energy, 71, 104619.

[14] Wang, Z., & Sobey, A. (2020). A comparative review between genetic algorithm used in com-posite optimization & the state-of-the-art in evolutionary computation. Composite Struc-tures, 233, 111739.

[15] Abbasi, M., Rafiee, M., Khosravi, M. R., Jolfaei, A., Menon, V. G., & Koushyar, J. M. (2020). An efficient parallel genetic algorithm solution for vehicle routing problems in cloud imple-mentation of intelligent transportation systems. Journal of Cloud Computing, 9(1), 6.

[16] Jatana, N., & Suri, B. (2020). Particle swarm & genetic algorithm applied to mutation testing for test data generation: a comparative evaluation. Journal of King Saud University-Computer & Information Sciences, 32(4), 514-521.

[17] Chen, X., An, Y., Zhang, Z., & Li, Y. (2020). An approximate nondominated sorting genetic algorithm to integrate optimization of production scheduling & accurate maintenance based on reliability intervals. Journal of Manufacturing Systems, 54, 227-241.

[18] Jain, G., & Prasad, R. R. (2020, June). Machine learning, Prophet and XGBoost algorithm: Analysis of Traffic Forecasting in Telecom Networks with time-series data. In 2020 8th Inter-national Conference on Reliability, Infocom Technologies and Optimization (Trends and Fu-ture Directions)(ICRITO) (pp. 893-897). IEEE.

[19] Lu, X.; Pan, Z.; Xian, H. An efficient and secure data sharing scheme for mobile devices in cloud computing. J. Cloud Comput. 2020, 9, 60.

[20] Yu, H.; Lu, X.; Pan, Z. An Authorized Public Auditing Scheme for Dynamic Big Data Storage in Cloud Computing. IEEE Access 2020, 8, 151465–151473.

[21] Chan, J.O.P. Digital transformation in the era of big data and cloud computing. Int. J. Intell. Inf. Syst. 2020, 9, 16.

[22] Ding, H.; Sun, C.; Zeng, J. Fuzzy Weighted Clustering Method for Numerical Attributes of Communication Big Data Based on Cloud Computing. Symmetry 2020, 12, 530.

[23] Daskevics, A.; Nikiforova, A. IoTSE-based open database vulnerability inspection in three Baltic countries: ShoBEVODSDT sees you. In Proceedings of the 2021 8th International Conference on Internet of Things: Systems, Management and Security

(IOTSMS), Gandia, Spain, 6–9 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–8.

[24] Ferrari, D.; Carminati, M.; Polino, M.; Zanero, S. NoSQL Breakdown: A Large-scale Analysis of Misconfigured NoSQL Services. In Proceedings of the Annual Computer Security Applications Conference, Austin, TX, USA, 7–11 December 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 567–581.

[25] Nikiforova, A.; Daskevics, A.; Azeroual, O. NoSQL security: Can my data-driven decision-making be affected from outside? arXiv 2022, arXiv:2206.11787.

[26] Thakre, B., Thakre, R., Timande, S., & Sarangpure, V. (2021). An Efficient Data Mining Based Automated Learning Model to Predict Heart Diseases. Machine Learning Applications in Engineering Education and Management, 1(2), 27–33. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/17

[27] Kumar, D. ., & Sonia, S. (2023). Resources Efficient Dynamic Clustering Algorithm for Flying Ad-Hoc Network. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 106–117. https://doi.org/10.17762/ijritcc.v11i2s.6034