Open Access Article

EFFICIENT SECURE DATA STORAGE AND DATA RETRIEVAL ON CLOUD USING MULTI-STAGE AUTHENTICATION FROM CLOUD DATABASES

Tunuguntla Kishore Babu
VTU-BELAGAVI (RESEARCH SCHOLAR), Department of Computer science and engineering, Karnataka, India.

Dr Guruprakash C
Sri Siddhartha Institute of Technology, Department of Computer science and engineering, Tumkur, Karnataka, India.

Abstract:
Cloud computing is becoming a major player in the information technology business as of its increased effectiveness, broad accessibility, low cost, and numerous advantages. It similarly offers additional storage capacity for Internet users and faster data transmission from one locality to another. Because of the large amount of storage available, cloud users can save a significant amount of money on IT infrastructure while focusing on their central business. As a result, a growing number of businesses and organizations are migrating to the cloud. However, due to security and privacy issues, many customers are hesitant to use the cloud. In a cloud computing system, all data is distributed across a network of remote servers and locations. Unauthorized cloud users gained access to this information via virtual computers. To address this issue, this paper proposes efficient secure data storage and retrieval system for cloud environment. To offer an additional level for cloud data security, this paper proposes authentication through encryption consuming public key cryptography, as well as multiple authentication-based data retrieval. The proposed Authentication Based Encryption approach contributes to better data security and cloud user authentication. The profound data is encrypted first and at that time secretly saved with the user's biometric finger print image. The resulting image is then transferred via an insecure channel. To prevent unauthorized access, the image is deconstructed and saved in the cloud distinctly as an encrypted message and a fingerprint. To improve system security, the encrypted and decrypted key value is appropriately selected using a search method. Following the encryption process, a data recovery procedure based on multiple security authentications is initiated. Unauthorized individuals will not be able to assault the data as a result of this. The proposed methodology's performance is executed, and the results are examined using several measures.

Keywords: Cloud Computing, Multiple authentication, Binary crow search, Biometric based finger print encryption

I. Introduction:

Cloud computing ensures widely regarded as one of the utmost important information technologies. As of resource virtualization, the cloud could offer on-demand self-provision, pervasive network access, quick resource resistance, and usage-based assessing, making cloud services as expedient as

Received: March 04, 2023 / Revised: April 22, 2023 / Accepted: May 28, 2023 / Published: June 15, 2023

About the authors：Tunuguntla Kishore Babu

Corresponding author- Email:

everyday efficacies like water, electricity, and gas. Despite its well- known economic aids, cloud computing gives users less direct mechanism ended the systems that achieve their data, raising substantial privacy and security distresses and serving as a major barrier to adoption.

Cloud computing (CC) own built significant progress in the automation business and scientific community in recent years. CC is a computational model that may be applied to any situation at any moment. They simply pay the amount dependent on how much they use it. Pay-as-you- go fashion is the name given to this strategy. In today's digital world, storage is also one of the furthermost important also necessary computing resources. In CC industry, it was one of the utmost widespread services. Many companies and industries keep their data in the cloud owed to the vast amount of storage available. Cloud data storage is well-known, with Amazon Simple Storage Service (S3) and Amazon's Elastic Compute Cloud (EC2), as well as Apple's iCloud. Security, on the other hand, is a big concern in cloud computing. With the advent of cloud computing, 3 types of cloud services have arisen: SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service).A variety of encryption techniques and access control systems have been devised to address the security issue. Confidentiality, integrity, and availability are the three points where security goals are specified. The confidentiality of data in the cloud is addressed through cryptography [1].

Cryptographic approaches should be used to fulfill data security in order to effectively handle security threats, as data encryption cave dwellers could provide important security aspects required by a cloud system. Cryptographic technologies, on the other hand, add added expenses to the cloud system (e.g., computing operational costs and memory requirements), reducing the cloud's economic benefits [2]. As a result, one of the most important tasks is to suggest realistic cryptographic algorithms for given that security sureties in cloud computing. While cryptographic techniques can meet the security objectives of a cloud system, they may suggestively decrease the cloud system's effectiveness, making typical data consumption service adoption complicated. For example, once the server implements de-duplication to excluding storage capacity, the usual cryptography of cloud storage yields duplication ineffective. Furthermore, due to data privacy protection, encrypted data could be started searching in the traditional manner, resulting in increased costs for both the user and the server. As a result, cryptographic approaches to achieving security goals that do not making favorable operational costs on the cloud system are preferable. This paper will focus on data storage and retrieval [3].

The total amount of data on the planet, according to the IDC, will exceed 40 trillion gb of space by 2020 [GD12]. Outsourcing data storage is an instance of a reflective cloud application. Both households and corporations store their data on the cloud to save time and money, reducing storage management exertion and enabling for far more adaptable data usage. Apart from eradicating this need local storage management; cloud storage is meaningless unless it can be recovered convenient and secure for use. In this work, we also attempt to gain data searching and transmitting for cloud data retrieval [4].

The proposed methodology's major goal is to use Authentication to safely send data to the cloud. The suggested approach is based on two layers of security: multiple authentication based access control and cryptography method. If any Stage Client provides incorrect information during the authentication process, he will be rejected instantly. As a result, no one other than the storage center's employees can access the data. Data is encrypted using a key when the authentication procedure is completed. Using the binary crow search algorithm, the key values are optimally selected (BCSA) [5].Finally, if the user passes the several authentication steps; the data is returned to them. Unauthorized users are avoided in such way. The continuing part of the article is systematized as follows: Section 2 goes on to discuss relevant research, Section 3 describes the suggested secure data transaction, Section 4 contextualizes secure data retrieval, Section 5 presents experimental findings, and Section 6 comes to the conclusion.

II. Related Work:

Much research had been conducted to secure data exchanges in the cloud. Cheng et al. (2018)[6] established a Personality Cryptography based personally liable confidentiality technique on CC, and is one of the studies mentioned here. At first, a held to account confidentiality method is done depending on the confidentiality characteristics.

Second, the suggested responsibility for CC includes a privacy-protection mechanism, as well as accounting and auditing methods. The proposed methodology's experimental results are assessed using several metrics. Another researcher used an indicator quasi-identifier strategy to establish a safe owing to its ability transaction in the cloud in Sudhakar and Rao (2020)[7]. For this experiment, they used an incremental and distributed data set. Brindha[8] and Shaji (2018) devised a particle-based conditional source trust attributes encryption technique. Secure cloud data transaction based on swarm optimization (CSTAE-PSO). The PSO algorithm was created in order to achieve the smallest transaction with the shortest completion time. The suggested methodology's performance was evaluated using several measures, including transaction throughput, data layer security rate, and transaction completion time output. Data is safeguarded with the use of bucketization to prevent sensitive data loss.

Pournaghi et al. (2020)[9] described the development of a block chain and attribute-based encryption. They safely store medical data on the cloud in this paper. A fine-grain access control method is used to prevent unwanted users from logging in. Suathi (2020)[10] also formed a cloud-based data protection system. This report discusses security issues by incorporating Altered Random Fibonacci Cryptographic techniques with Session Key Premised Attribute Encrypted data (MRFC). This input data existed originally kept separate as sensitive and non-sensitive information exhausting the attribute separation method. The confidential material is then encrypted using MRFC. This method's efficiency is evaluated to use a variety of measurements. Suresha and Karthick (2020)[11] proved data protection using the Threshold Cryptography Technique. This method takes into account data security concerns there into cloud service further effectively. In this approach, this same Data Access Control can also be used to regulate access to data. The proposed method helps protect data more effectively, increasing system performance and cutting the number of secret keys.

Kali et al. (2019) health record deal was formed to use a block chain method. This work in healthcare makes it easier to control and stake a patient's medical database in cloud storage while maintaining privacy. This is an excellent way for intelligent healthcare systems to personalize patient data. Shen et al[13]. suggested a wireless body area network authentication protocol that is lightweight, certificate-less, and cloud-assisted. This protocol, with the exception of the network manager during the registration process, serves to verify the user's true identity. Santosh[13] and his colleagues created an

RSA-based method for cloud data security. When analyzing the method, they looked at space complexity, time complexity, and throughput. The RSA algorithm ensures data security thru restricting access to simply the rightful possessor of a data. Sasi and colleagues developed a biometric method that combines fingerprint with iris recognition. The minutia matching method is used to equate the image by percent level. It likewise offers access control and authentication for secure allocation .The multi-prime RSA algorithm was developed by Sunanda et al[14].

We have many security based algorithms on image steganographic methods to strongly conceal consumer's secret data. Sharma V et al. suggested a novel procedure for storage user data in a cloud environment exhausting image steganography then image cryptography methods. In whichever privacy information is encrypted expending the DES algorithm and a protected key is obtained, which is then encoded using the S-DES algorithm. So the absolute one is engendered using the S-DES algorithm, which hides the key in designated pixels to cover image. The consequences are virtuous, and it offers great security by adequate PSNR values. Yousef Bani et al. projected an algorithm aimed atwalloping secret data in an image consuming genetic then blowfish algorithms in Inability.

III. Proposed work:

Cloud computing is a service that has seen explosive growth in recent years in the information technology industry. Cloud users and suppliers face difficult concerns with privacy and security. Users in a public cloud environment have no control over their distant data when it is sent to a public cloud server. As a result, data security, such as confidentiality, integrity, availability, and dependability, is a major concern in public cloud storage. This study proposes authentication as a solution to this problem. Its goal is to improve the security of sensitive data stored in public cloud storage. Multiple authentications, data security utilizing secret key and query-based data retrieval are the three stages of the proposed method. SaaS is used in this manner. This strategy protects data from both insider and exterior threats.

Registration, secure data storage, and retrieval are the three stages of the proposed methodology. During the registration phase, users register their information in the cloud. To avoid an unapproved person using the login process during this phase. During the security step, the information is secure using the Blowfish technique and saved in the registered user's fingerprint image. To improve the blowfish, the encryption keys are chosen optimally spending the BCSO technique. During the recovery phase, accredited personnel send the request for server. The data will be sent to the registered user; otherwise, the request will be ignored.

Registration Process:

Clients arrived with their info on the data center at the registration step. To begin, the client produces a user id Uid and a password Pid, as well as entering all of the user's data. The user register fingerprint image also. Finger print of the registered user image then submitted to the server and saved. The neatly trimmed region of the selected image is then supplied to the domain controller to enhance authentication. This information will be deposited on the server. Figure 1 shows the registration process of the user.

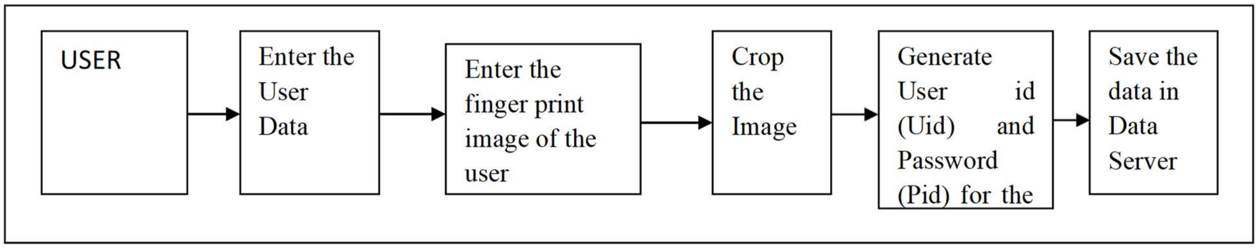

USER
Enter the User Data
Enter the finger print image of the user
Crop the Image
Generate User id (Uid) and Password (Pid) for the
Save the data in Data Server

Figure1: User Registration Process

The customer can publish and download data to the cloud after successful registration. Neither customer can access the cloud first without registering. By using this method, we can avoid loss of data. In asked to register in, clients should first submit their details, including such their user id Uid and passcodes Pid. The made explicit the information after having received it. If it is accurate, the host will ask the user's fingerprint template right away. The registered picture and the current picture are compared. The process continues since this image is identical to the registered image. The user's application will be ignored otherwise. Following the image selection procedure, the customer yields same image.The server then needs to be compared the entered finger print image to the pre recorded neatly trimmed image. If the request matches, the server permits the client for access a data; else, the request is ignored. Figure 2 shows the registration process after entering the biometric fingerprint image .

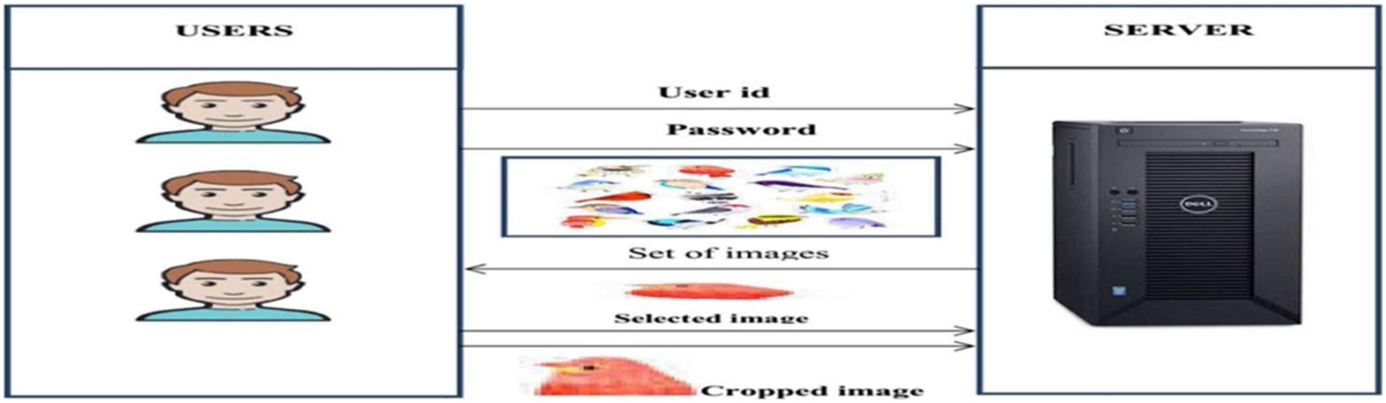


Figure 2. Complete Registration Process

Secured Data Storage:

The cloud user strives to just save plain data (D) in an encrypted message that use the Blowfish technique's key pair (or) private keys (ek) (DC). The Blowfish algorithm is probably more suited to making sure data transfer and storage security. Invaders who have not had right to possession are still unable to access this same plain data. Unauthorized access cloud users have already had access to data on occasion. To address this issue, biometric authentication, including such finger prints, is used to prevent unwanted access to sensitive information. The encrypted data was hidden with the original data's owner's fingerprint recognition (SImg) and then sent to cloud storage. The raw data as well as the image of a finger print are detached.

The basic data and the thumbprint image are broken down into separate clumps. The plain data will be implanted into the alterative location of the bounding box to start generating an embedded image (IDC), which will be sent over to cloud storage. The IDC was split by the Cloud Service Provider in to the fingerprint images (SImg) and encrypted (DC) (CSP). Eventually, the above information has been decided to add to the authorization table.
This table includes 2 pastures, including one that stores the finger print photo (SImg) acquired since of the holder for plain data (the "Image field") and alternative of which points to the position of cypher data (DC) (the "Data field"). If indeed the finger print image already persists in the table before storage, the cypher information (DC) is concatenated to the authorization table's data field. Or else, both authorization table fields are modified. This stall aids in the confirmation of cloud authentication process via fingerprints. The blowfish method is being enhanced using the optimum solution key method of selecting. In this article, the BCSO method is used to start generating a key. The crow search algorithm is a newly invented inventive meta-heuristic complex calculation based on crow behavior and attitude and knowledge.
Data Storage Algorithm

Simple data as input (D)
Cipher Data is hidden with a finger print image as an output (IDC) Step 1: Read the raw data (D)
Step 2: Using the BCSO algorithm, generate a key.

keys are classified into two types: encryption keys (ek) and decryption keys (dk) (dk)

Step 3: Encrypt the simple data (D) with "ek" (i) Split the data into DBi blocks with i=1,2,3,...n (ii) Encryption produces blocks of cypher data DCi, where i=1,2,3...n.
Step 4: Deliver the image in cloud user's finger print (SImg). Step 5: Keep hiding DCi in the finger print image.
Step 6: IDC uploads the results to the cloud.

Data Retrieval:
Formerly when encryption process is done, this encrypted data is saved into cloud. If a user requests data which has already been stored, they must first make aentreaty to the CSP. A CSP performs various verification where the processor verifies user information. If the data supplied is precise, the user is accorded contact to all data. Or else, the entreaty will be dismissed.
In our proposed data retrieval architectural style, we use Double Pki Encryption with Keyword Search (DS-PEKS). DSPEKS includes (KeyGen; DS-PEKS; FrontTest; DS-Trapdoor; BackTest). Rather than the public/private key pairs to receiver, the KeyGen process yields the public/private shared key for front and back servers. Moreover, the secret door formation algorithm DS-Trapdoor mentioned now is available to the public, although the Secret door algorithm in the quintessential PEKS description requires the recipient's secret key as insight.

The structures of the two systems differ, actually results in such a discrepancy. As there is only one server in quintessential PEKS, the host can recover a keyword cipher - text by trying to conduct an online taking a guess attack if the secret door basic prerequisite is known.

Another difference among regular PEKS and the suggested DS-PEKS is with testing method is split into 2 parts: FrontTest and BackTest, that are path by 2 distinct servers. When itwas forced to defend against interior keyword going to guess attacks. When front server receives a question from the recipient, it utilizes its secret key to pre-process the trapdoor and all PEKS cipher texts before having to send some extensive testing to the rear server while trying to conceal the trapdoor and PEKS cipher texts.

Algorithm:

Step 1: Generates the system parameters params using the security parameter user id and password as input.

Step 2: The second step is to generate a key. Returns the public/secret key pairs (pkFS; skFS) for a front server and (pkBS; skBS) for a back server based on the set parameters params.

Step 3: As hyper parameters, it takes front server's public key pkFS, a rear server's public key pkBS, and a search term kw1 and needs to return the PEKS ciphertext CTkw1 of kw1.

Step 4: DS-Trapdoor(params; pkFS; pkBS; kw2): Takes parameters, the public key pkFS of the front server, the public key pkBS of the back server, and the search term kw2 as inputs and outputs for trapdoor Tkw2;

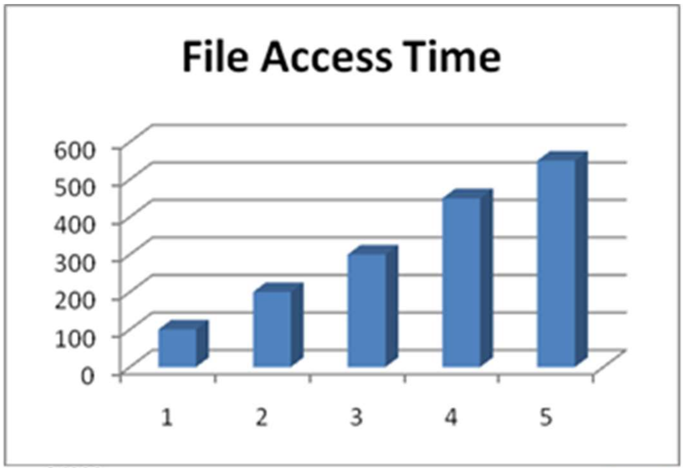
Step 5: FrontTest(params; skFS; CTkw1 ; Tkw2): This function that proceeds as input parameters the front server's private key skFS, a PEKS ciphertext CTkw1, and an trapdoor Tkw2, and returns the core testing-state CITS.

Step 6: BackTest(params; skBS; CITS):Receipts params, the private key skBSfor back server, and the core testing-state CITS as input data and needs to return a 0 or 1 for the experimental results.

IV. Results:

The performance for proposed research methods was measured as units of file access time, retrieval time, decryption time, encryption time, and memory usage. The chief objective of the suggested method has securely send data into cloud starved of having any problem. To achieve this, an inventive multifactor authentication method and data encryption automated system is used. The graphs show the consequences of the proposed method. Figure 3portrays the proposed methodology's performance in expressions of file access time.

The x-axis signifies the file size, and the y-axis (10, 20, 30, 40, 50) signifies the time. According to Fig. 4, the proposed method accesses the 10 kb file in 55 milliseconds. Figure 4depicts the performance for proposed approach in rapports of encryption time, while Figure 5 depicts the performance in rapports of decryption time. The proposed solution also kept the encryption and decryption processes to a bare minimum. Figure 6 shows how the proposed strategy performs in expressions of memory. In such case, when a file size increases, so does the amount of memory used. Sending 40 kb of data requires 15,359,766 bits of RAM, according to Fig. 8. It's only a formality.



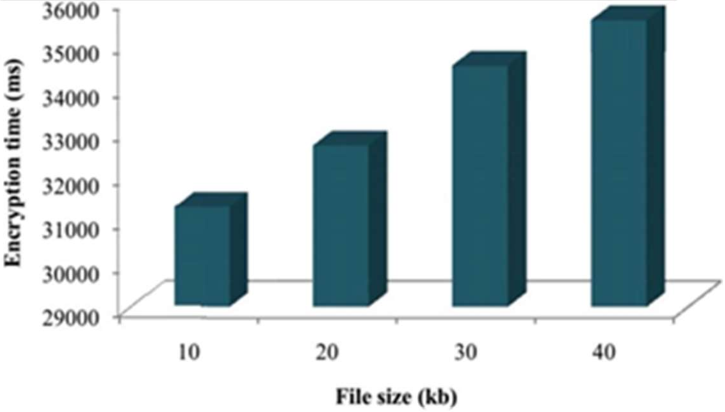
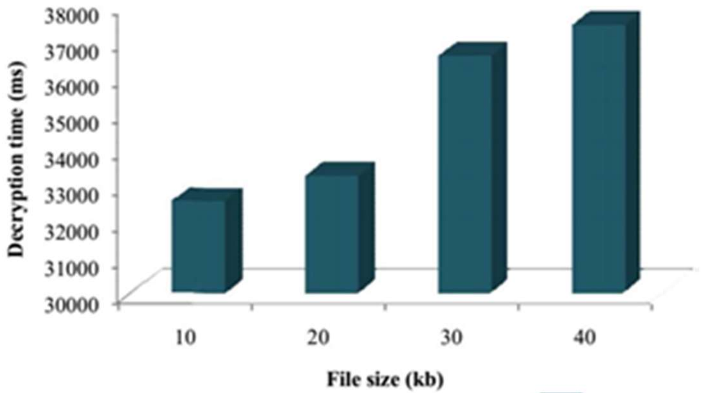


Fig. 3 Performance of the proposed method based on file access time Fig. 4 Performance of the proposed method based on encryption time



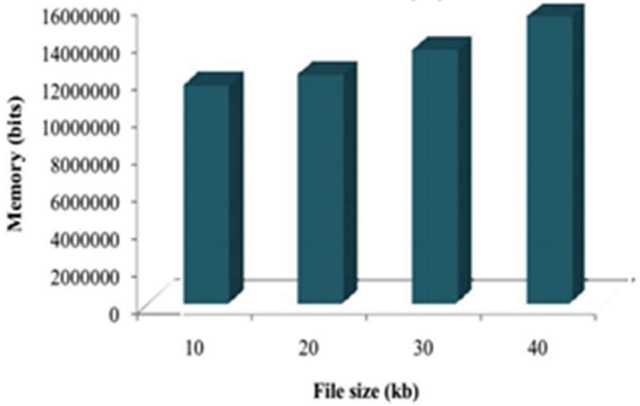


Fig. 5 Performance of the proposed method based on decryption time

Fig. 6 Performance of the proposed method based on memory

Due to the magnitude of the encryption and decryption keys, Table 1's data retrieval time is marginally longer than data storage time. Sometimes, the roles may be reversed. The suggested method is divided into two sections: encryption and embedding cypher data (DC) into a finger print image (SImg).

Table.1.Contrast of data storage and retrieval between RSA and Proposed Algorithm

File Size(KB)	RSA		Proposed	
	Data Storage Time(ms)	Data Retrieval Time (ms)	Data Storage Time (ms)	Data Retrieval Time (ms)
10	23705	23911	25493	25748
20	31924	31825	33439	33561
30	40233	40746	42139	43668
40	55864	52948	57324	57759
50	62541	62744	64431	64553

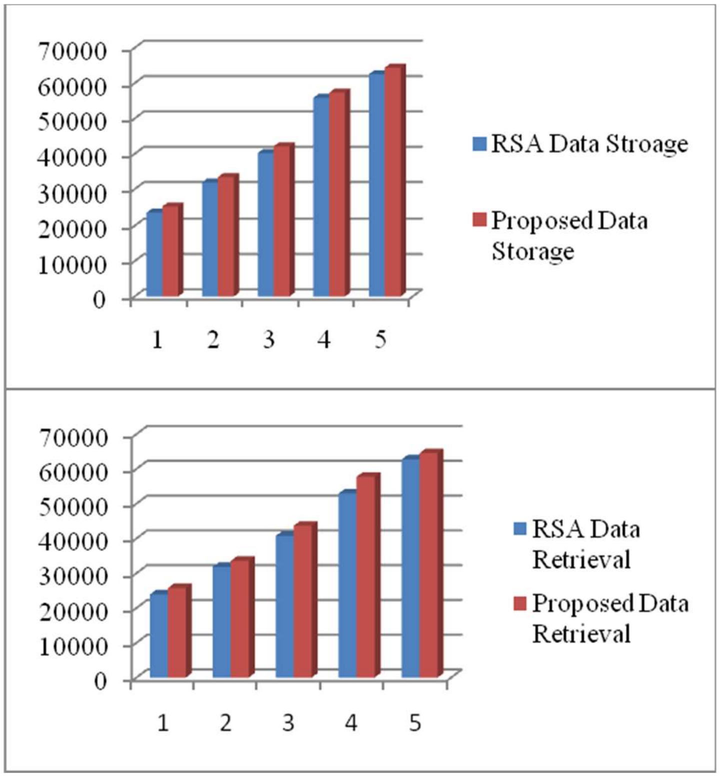


Fig.7.Comparison of Data storage and retrieval time

Computation Costs: All previous systems require pairing computation during PEKS cipher text creation and testing, making them less effective than our technique, which doesn’t necessitate pairing computation.

V. Conclusion:

Cloud computing is a popular new technology. The cloud service has provided greater benefits to users, particularly large businesses. To reap the benefits of cloud computing, secure data storage is even more critical. Anyone can store and access data on the public cloud. In the cloud, there is no access control or security. The suggested approach uses biometric authentication to ensure access control and uses public key cryptography to address security concerns. The CSP keeps track of the data owner's fingerprint in the authentication database. The results of the speed study, like retrieval time and data storage, demonstrates that the suggested strategy performs enhanced. Any transformation in file size has an impact on performance for cloud storage service. Data access is not feasible unless an appropriate finger print image is sent. It makes things simpler to progress the data security in the cloud platform. The price of data storage with retrieval would need to be investigated in the future. Furthermore, in order to enhance efficiency, the public key cryptography algorithm's execution speed should be improved.

References:

1. RajkumarBuyya, James Broberg and Andrzej Goscinski, “Cloud Computing Principles and Paradigms”, John Wiley and Sons, Inc, 2011.

2. Bisong, A. and Rahman, S.S.M. (2011) “An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, Vol. 3, Issue 1, Pg. 30-45, 2011

3. Dinesha, H. A., & Agrawal, V. K. “Multi-level authentication technique for accessing cloud services” In 2012 International Conference on Computing, Communication and Applications (pp. 1-4). IEEE, Feb 2012

4. Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y, Cloud-aided lightweight certificate less authentication protocol with anonymity for wireless body area networks. Journal of Network and Computer Applications, 106, 117-123, 2018.

5. Santosh Kumar Singh, Dr. P.K. Manjhi, Dr. R.K. Tiwari, Data Security using RSA Algorithm in Cloud Computing, International Journal of Advanced Research in Computer and Communication Engineering,Vol. 5, Issue 8, Aug 2016

6. D. Boneh, G. Crescenzo, R. Ostrovsky, G. Persiano, Cheng “ Public Key Encryption with Keyword Search”, Proc. International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt), 2018.

7. R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, Sudhakar “Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions,” Proc. ACM 13th Conf. Computer and Comm. Security (CCS), 2020.

8. O S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, “Zerber+r Brindha: Top-k Retrieval from a Confidential Index,” Proc. 12th International Conference on Extending Database Technology: Advances in Database Technology (EDBT), 2018.

9. A. Swaminathan, Pournaghi Y. Mao, G.-M. Su, H. Gou, A.L. Varna, S. He, M. Wu, and D.W. Oard, “Confidentiality-Preserving Rank-Ordered Search,” Proc. Workshop Storage Security and Survivability, 2020.

10. C. Wang, N. Cao, K. Ren, W. Lou, Suathi “ Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data”, IEEE Transactions On Parallel and Distributed Systems, Vol. 23, No. 8, August 2020.

11. P.S. Priya, D. Preethi, J. Priya, B. Shanthini, Suresha and Karthick “ Retrieval of Encrypted Data Using Multi Keyword Top-k Algorithm”, International Journal of Scientific and Research Publications, Vol. 4, Issue 4, April 2020.

12. P. Akriti, P. Mary Ann, D. Sarvanan, Kali " Ranked Keyword Search Using RSE over Outsourced Cloud Data", IPASJ International Journal of Computer Science, Vol. 2, Issue 3, March 2019.

13. Shen D.Song, D. Wanger, and A. Perrig, "Practical Techniques for Searches on Encrypted Data" Proc. IEEE symp. Security and Privacy, 2020

14. Sunanda B.Reddy Kandukuri, V. Ramakrishna, A. Rakshit, "Cloud Security Issues", 2019 IEEE International Conference on service computing(SSC 2019), September 2019, Bangalore. pp. 517-520