AN EFFICIENT KEYWORD SEARCH AND DATA SHARING SCHEMES IN CLOUD COMPUTING

[#1]AATIKA FATIMA, M.Tech Student, Dept of CSE,

[#2]Dr. SRINIVAS REDDY, Associate Professor, Dept of CSE

[#3]Dr.CHANDRAMOULI NARSINGOJU, Associate Professor & HOD, Dept of CSE

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TS.

ABSTRACT:

Hardware and software resources in computing infrastructure have become much less expensive as a result of the expansion of cloud computing. For the purpose of keeping the data secure, it is encrypted before being transferred to the cloud. Once the data has been encrypted, it is nearly hard to locate and share it with others. Even However, even while customers desire that the cloud deliver search results quickly while also keeping their data secure, the search service provider is responsible for ensuring that this function is fulfilled. In order to address these issues, we propose an attribute-based solution that incorporates keyword search and data exchange techniques (CPAB-KSDS). Due to the addition of support for attribute-based keyword search and attribute-based data sharing, this technique goes above and beyond the capabilities of already available keyword search and data sharing systems. Additionally, we may make a keyword modification while the distribution step is still in progress without having any impact on the PKG. The entire purpose of this work is to introduce the concept of CPAB-KSDS and its associated security model. A strategy is also shown, and its effectiveness is demonstrated using either a random oracle model or through the use of a keyword attack. It was demonstrated to be both practical and efficient, hence demonstrating the feasibility of the suggested concept.

Keywords: Cloud storage auditing, cloud storage, outsourcing computing, key update, encryption.

---

1. INTRODUCTION

Cloud computing makes it feasible for multiple different applications to access the same resources at the same time, provided that they all make use of cloud computing. Users are now able to store, retrieve, and share their data more simply as a result of the advent of cloud computing. This service is advantageous to both the individuals who utilise it and the businesses who provide it. This type of flexible structure is ideal for getting work done whenever and wherever you need it. It provides low-cost services, upgrades your software for you, and encourages teamwork among its employees. The most widespread acceptance of cloud storage has been for usage in the cloud, which has received the most attention. It is common for people to use cloud storage on a regular basis to store significant amounts of data. In order to safeguard sensitive information from cyber threats, an additional layer of protection must be implemented. Encryption techniques are available in a variety of formats and are used to protect sensitive information from prying eyes while also ensuring the secrecy of data. The deciphering of encrypted data proved to be a difficult task. A user would do this by typing in a search word and searching for a corresponding file. With keyword searching, it is tough to search entirely based on whether or not you know the

specific keyword you're looking for. The recent advancements in fuzzy keyword searching, such as the use of ranking functions that rank sets of keywords for inclusion in searches, may allow researchers to use this technology to search for encrypted files even when the keywords are spelled incorrectly or misused, while also maintaining the privacy of the keywords themselves. The researchers Shekokar et al. created a server-based keyword search that makes use of wildcard technology to get relevant results. In the context of cloud security and data protection, authentication and access control measures are employed. Database management systems (DBMS) make use of cloud-protection technology to keep their data safe. Only effective security control methods are activated if the server is assessed to be secure in the first place. The majority of the time, however, the techniques meant to restrict access are ineffective in this situation. The cloud server must be dependable and validated in order to ensure the security of user data.

CLOUD SERVICES, ISSUES AND REQUIREMENTS

CLOUD SERVICES

Cloud networks are more vulnerable to security breaches than any of the organisations to which they are connected. According to this source, cloud computing is comprised of three fundamental components.

User: Users of cloud computing service providers Individual clients, corporations, and other organisations all receive the same level of service and consideration. They don't have to be concerned about remembering all of their personal information in their heads any longer.

Cloud Service Provider: This body maintains control over and provides users with critical resources and knowledge through a network of regional servers.

Third Party Auditor: In order to assist users in utilising cloud services when they are unable to do so on their own. You are free to include it if you so desire.

CLOUD SECURITY ISSUES

Despite the fact that cloud services offer a number of advantages, many organisations and individuals choose to forego these benefits in order to avoid heightened security risks. The following security risks were identified and discussed:

Data breaches: It is possible for users' most secret and sensitive information to be stolen or viewed by unauthorised parties when they use cloud storage services. Furthermore, everything from trade secrets to health information and more is covered.

Account hijacking: In order to gain unauthorised access to a user's cloud data, a hacker first has to obtain the user's login credentials from the user. The hacker then uses the credentials obtained from the user to carry out illegal or malicious operations on the cloud data of the user, as described above.

Insider attacks(threat): User data, such as financial forms, account information, and other sensitive information, is obtained illegally by an employee who has been authorised access to the relevant skills in an organisation. The majority of the company's efforts are devoted to preventing external threats, rather than dealing with this specific problem.

Malware injection: Saas, which is an abbreviation for "software as a service," is now infected with malicious viruses or scripts that might cause harm. When malware is installed on these contaminated systems, the "legitimate instances" that they are used to convert become "compromised genuine instances." While it appears to be doing nothing more than what is natural to outside observers, it actually makes it easier for hackers to steal valuable information.

Denial of service attack: In order to deny legitimate users access to the system, an attack will seek to overload the network, the system, and the services to the point where access is denied to valid users who have been granted access.

Data loss: The effects of natural disasters, such as earthquakes, might result in data loss as a result of the earthquake itself. While the organisation may

have a backup policy in place, it is possible that the data is not being handled and managed in an effective manner on a cloud server.

Insecure APIs: APIs are used by developers to customise cloud-based services in order to fulfil the needs of businesses. Because of the enhanced infrastructure, it is now more likely that a security breach will take place. When an application interacts with one or more APIs, the security of the application is a major consideration.

CLOUDSECURITY REQUIREMENTS

A large amount of data protection is still required due to the ongoing upkeep required by cloud computing. It is impossible to overstate the importance of developing trust between users and service providers. In order to be considered secure, the cloud infrastructure must be capable of enforcing security measures within its own premises.

To safeguard cloud-based data, the following additional security measures must be taken:

Authentication: Using this method, individuals can work toward the aim of developing their own identities while also ensuring that they are speaking truthfully. As a further security measure, any future communication channels cannot be impersonated by any unauthorised third party, such as a service provider, thanks to the solution's use of encryption.

Access control: Depending on the security requirements in place, segregation can be an effective strategy for controlling access to systems and applications. The identification and authentication of the entity that will be allowed access privileges are critical for the time being.

Confidentiality: Keep private cloud data out of the reach of unauthorised individuals is crucial for maintaining secure secrecy in the cloud. With the exception of specific banned elements, the assailant is not allowed to examine the frequency, length, and other network-related features of the communication.

Integrity: Every piece of data that passes via the network has been validated and is correct. Receiving data that has been altered or manipulated is strictly forbidden. Making alterations is restricted to those who have been granted the power to do so.

Availability: Because of this service, authorised users may be assured that the information they seek will always be available.. In order to protect against Denial of Service attacks, system backups should be performed on a regular basis.

Non-Repudiation: In this service, the senders and recipients are both checked to ensure that the information was delivered and received properly. Accurate and verifiable documentation is required in order to complete this task successfully.

2. REVIEW OF LITERATURE

A secure attribute-based data sharing mechanism has been developed for cloud computing customers who have limited resource availability. The proposed approach has the potential to increase the data sharing capabilities of mobile users who have restricted resources in cloud computing. It is recommended by the system's developers that they include open system settings, outsource some encryption work to the cloud, and incorporate other features to make their new system more desirable. The security of an adaptive selected ciphertext attack is demonstrated under the proposed approach.

a cloud-based network in which patients' anonymized health data is exchanged and used in the electronic health record (EHR) People are unsure if public cloud servers can be trusted, which leads to a large amount of data being kept on them. When it comes to sensitive data, security and privacy become even more critical considerations to take into consideration. According to the findings of this study, a new and more secure technique to share data without disclosing the information of the data owners can be established while still ensuring the privacy of outsourced cloud data. It allows for greater freedom in the use of data while simultaneously taking into consideration considerations such as

privacy and security. Using this proof of concept, we can see that the proposed approach is feasible and efficient. In the final section, we'll talk about how the concept relates to electronic health records.

When searching for public key encryption, keywords are used as search terms. In terms of the process of looking for encoded data, we believe that having an open key system is a smart practise. Consider the following scenario: Bob, a customer, sends Alice an email. When he combines their emails, he places them all in a single folder under Alice's "Open" key, which she can access from any computer. It is vital to have a user-friendly email gateway in place in order to ensure that emails containing the term "sincere" are appropriately logged. It is possible to see mail servers from a different perspective than the one described above: Regardless of whether a letter is being sent, they all contain the same slogan in them. In order to demonstrate open key encryption, we present the additional features that a person may be able to request when asking the encryption password.

It is a lightweight and effective cloud computing data sharing solution that uses cloud computing technology. ABE is frequently used in dispersed environments, such as cloud computing, to ensure the security of data communication. Methods developed by Abe can only be employed in a cloud setting with limited resources. Using the technique described in this work, encrypted data storage may be delivered on EC-enabled cloud storage systems. In light of the fact that our technique is both safe and productive, we strongly encourage you to put it into action.

To make data sharing possible, we must make use of the Secure Keyword Search tool. By utilising cloud computing technologies and data sharing, this method adds a ciphertext-policy characteristic to cloud data, allowing for more secure cloud data storage (CPAB-KSDS). Instead, the suggested solution provides attribute-based keyword search as well as attribute-based data sharing, in contrast to the current systems, which only allow for one of these characteristics to be enabled. In this strategy, there is no need to do anything to keep the term up to date. This paper delves into the concept of CPAB-KSDS as well as the security model that underpins it. The investigation is carried out using a selected ciphertext attack and a selected keyword attack. Both of these attacks are employed, with the assumption that the oracle is a random oracle in both cases.

Anonymous hierarchical identity-based encryption, also known as hierarchical identity-based encryption, is accomplished by the use of anonymous hierarchical identity-based encryption (also known as AHIB). In this demonstration, we will employ a ciphertext-based cryptosystem that makes use of completely opaque ciphertexts and multiple levels of key distribution. If there is no other option, please go ahead with the procedure as planned. The assumption that the linear complex nature presumption is accurate provides justification for conventional model security. This strategy is very effective and advantageous since it produces basic cypher messages that hold considerable information about the chain's relevance while remaining simple and straightforward. Information applications make it possible to access personal information, encoded data, and completely private correspondence from anywhere at any time. In response to the first inquiry, a positive conclusion indicated that two obscure character-based encryption arrangement concerns had been resolved.

Several organisations with superior security are joining together as part of a wider joint endeavour. This design makes use of the Symmetric Balanced Incomplete Block Design technique (SBIBD) Cloud computing is addressed in this research, which addresses new and diversified collection methods on the cloud while keeping a high level of security and effectiveness. In order to take advantage of the understanding, a new information collection and sharing mechanism has been implemented. This way will be especially beneficial for clients who like to keep their business activities under wraps. In the pro key

age, a symmetric modified fragmented square construction is used as a foundation (i.e., due to employment of this, there is less of a stress on people to discover a typical gathering key). The efficacy and security of the established approach are validated through the use of distributed computing, which performs hypothetical tests and examination exams.

It is critical to employ realistic approaches while attempting to decrypt encrypted information. A security risk is the possibility that personal information, such as personal e-mail accounts and private work documents, will be stolen or compromised. As a general rule, security is sacrificed at the expense of overall usefulness. Take into consideration the following: A client is only interested in retrieving archives that contain phrases that they have searched for. The information hoarding server must determine which search keywords to look up and which information to send to the consumer in order to create these archival collections.

3. RELATED WORK

In an ABE, users are represented as a list of properties that can be accessed by other users. After Abe completed his research, other scholars built on his findings to further establish the concept of ABE. A cryptography private key is associated with an access policy, which assigns a ciphertext attribute set to each user based on the private key. The relationship between the ciphertext and the access policy is due to an attribute set that is utilised in CP-ABE to generate the private key.

Furthermore, for both KP-ABE and CP-ABE, the length of the ciphertext and the size of the access policy are inversely proportional to one another. It was policy-based ciphertext length that was utilised for the first time, according to Emura et al. [8, in the case of the first use of a ciphertext length property]. This attribute and gate adapter allow you to use expressions that are not monotonically connected, but they do not accept monotonically connected expressions. Numerous new structures have been built since then to improve efficiency, security, and expressiveness while also reducing costs and increasing productivity. According to the findings of the research by Li et al., attributeteless encryption is used in the PHR system to manage access to personal health records with fine-grained degrees of access control, and this is demonstrated in the PHR system.

An attribute-based policy encryption system with disguised policy was proposed for the PHR system, with the disguised policy being used for privacy considerations. It was rejected. It is possible to decrypt encrypted messages on a mobile device with limited processing power by using outsourcing decryption attribute-based encryption. In some cases, even while the service provider is able to offer the right partial decryption ciphertext, this does not guarantee that the operation will be successful. The attribute-based encryption system was developed by Lai and Li (14 and 15) in order to address this problem. The system incorporates outsourced decryption methods that have been verified, which serves as an additional degree of protection. It was created in order to allow for the delegation of decryption to be possible. In the past, research has concentrated on the operation, efficiency, and security of computer systems.

In a 2011 study, Liang et al. (21) developed a proxy re-encryption strategy that they used to an attribute-based configuration re-encryption instance, which they called the attribute-based configuration re-encryption instance. This separate AB-PRE architecture was created in order to make AND gate operations on both positive and negative values more convenient to perform. The monotonic access formula proposed by Liang et al. [23] is used to grant ciphertext proxy access to an attribute-based ciphertext proxy system that they have developed. An adaptive strategy has been used to implement a greater level of security in the following years.

The security provided by these two KPABE systems [25,26] can be used by both the selective and adaptive models [25,26]. Earlier this year, Liang and colleagues (27) published a work in the journal Quantitative Structure Analysis in which they suggested a deterministic finite automata (DFA) based PRE technique. When it is treated as a DFA, the access policy is applied in accordance with the law.

Using this search option does not require the collection of any personal information. Another option that has begun to gain in favour is the inclusion of search capabilities in public key encryption. This is a relatively new development. In a symmetric key encryption environment, Song et al. [28] discovered the primitive of searchable encryption and proved it to be correct. Following the conclusion of their research, more searchable encryption systems were demonstrated that included a variety of features such as a keyword ranking search and a keyword fuzziness search among others. an approach for searching for keywords that makes use of public key encryption is described here (PEKS).

In TCC 2007, Boneh and Waters proposed the PEKS technique, which allows for keyword queries that include a range, subset, and conjunctive query. This is the next stage in the keyword research process, which is also known as attribute-based keyword search. Data owners are used to issue keys to data consumers in an efficient attribute-based searchable encryption system, which is based on attribute-based searchable encryption. A keyword search system was developed in shared multi-user contexts that included attribute-based policy and could be used by multiple users at the same time. Despite this, none of the data exchange types specified below could be used to implement the functionalities because none of them were available.

A keyphrase search mechanism was developed in order to allow a server to locate certain ciphertexts and re-encrypt them when necessary.

If an ABE-based key policy is used, this PKG keeps the data owner's authority to give access policies in tact; on the other hand, the encrypted data owner loses that same authority. It is critical to emphasise that, in a PHR system, the owner of the data has complete control over the information. This follows naturally from the prior illustration. As a result, adopting a ciphertext policy with attribute-based encryption, keyword search, and data exchange is the most effective method available. Additionally, the PKG will need to request that the data owner produce a search token, which will necessitate the data owner putting out additional effort. Additionally, data should be supplied to PKG delegates so that they can pass the information on to their delegates who are not a part of the organisation. Due to the fact that PKG was unable to assist with this project, they decided to leave it as an open challenge, daring individuals or organisations to utilise an attribute-based encryption technique to create a dataset that is searchable and shareable without the assistance of PKG

4. RESULTS

In our testing, we used eight different search encryption schemes, all of which were novel at the time of the testing: a keyword search technique based on the attribute idea [35], a recently developed attribute-based keyword search method [34], and a KPAB-PRE-KS implementation.

TABLE I
FUNCTIONALITY COMPARISON WITH [30], [34], [35], [36].

Schemes	Keyword Search?	Data Sharing?	Access Policy	Without interactive with PKG?	private key or public key setting?
[30]	✓	×	×	✓	private key
[34]	✓	×	Ciphertext policy	✓	public key
[35]	✓	×	Ciphertext policy	✓	public key
[36]	✓	✓	Key policy	×	public key
Ours	✓	✓	Ciphertext policy	✓	public key

TABLE II
COMPUTATION COMPARISON WITH [30], [34], [35], [36].

Schemes	Enc	TokenGen	Test	ReEnc	Dec(Dr)	Dec(Rc)
[30]	$O(\lambda^2)\cdot m$	$O(\lambda^2)\cdot m$	$O(\lambda)\cdot m$	$\perp$	$\perp$	$\perp$
[34]	$O(\lambda)\cdot\epsilon+O(\lambda)\cdot p$	$O(\lambda S)\cdot\epsilon$	$O(\lambda S)\cdot(\epsilon+p)$	$\perp$	$\perp$	$\perp$
[35]	$O(\lambda)\cdot\epsilon$	$O(\lambda S)\cdot\epsilon$	$O(\lambda S)\cdot p+O(\lambda)\cdot\epsilon$	$\perp$	$\perp$	$\perp$
[36]	$O(\lambda S)\cdot\epsilon+O(\lambda)\cdot p$	$O(\lambda)\cdot\epsilon$	$O(\lambda S)\cdot\epsilon+O(\lambda)\cdot p$	$O(\lambda S)\cdot\epsilon+O(\lambda)\cdot p$	$O(\lambda S)\cdot\epsilon+O(\lambda)\cdot p$	$O(\lambda S)\cdot\epsilon+O(\lambda)\cdot p$
Ours	$O(\lambda)\cdot\epsilon+O(\lambda)\cdot p$	$O(\lambda S)\cdot\epsilon$	$O(\lambda S)\cdot(\epsilon+p)$	$O(\lambda M)\cdot(\epsilon+p)$	$O(\lambda M)\cdot(\epsilon+p)$	$O(\lambda M)\cdot(\epsilon+p)$

TABLE III
IMPLEMENTATION TIME.

Algorithms	KeyGen (ms)	Enc (ms)	TokenGen (ms)	Test (ms)	RKenGen (ms)	ReEnc (ms)	Dec(Or) (ms)	Dec(Re) (ms)
|S| = 5	12.954	40.003	7.232	16.171	51.667	33.914	9.463	31.640
|S| = 10	19.934	67.811	10.515	24.083	86.230	61.216	17.682	58.685
|S| = 15	26.146	98.433	13.810	32.006	120.610	88.598	25.720	87.315
|S| = 20	33.624	125.362	17.106	39.826	157.500	117.622	34.438	116.067
|S| = 25	40.479	152.616	20.392	47.753	191.435	142.800	42.745	141.702
|S| = 30	46.616	181.117	23.673	55.647	226.063	171.027	50.708	169.145

formulate and prepare [37] The process of reviewing the various points in this manner consists of taking into consideration three aspects: the functionality given, the theoretical analysis time of the algorithm, and the practical execution time of the algorithm in question.

A. Functionality Comparison

Based on the information in the table, we have data sharing and keyword search functionality built into our approach. Furthermore, our technique is applicable in both the public key and the private key environments. Every time the delegator wants to generate a new re-encryption key, the delegator must communicate with the PKG. As an alternative to developing an algorithm that generates the re-encryption key, which is required by the PKG, we have instead developed a system that employs the ciphertext-policy paradigm, which means that the PKG is not required to generate the re-encryption key, thereby alleviating the burden placed on the PKG by this requirement.

B. Efficiency Theoretical Analysis

Take a look at Table II for a short breakdown of the various computing charges that we've incurred. In Table II, the total number of characteristics in an attribute set is represented by the security value "," which is equal to the total number of characteristics in the scheme. A policy defines the total number of row numbers (M,). This is referred to as the total row numbers or just the row numbers in some instances. For example, the cost of a group G or GT calculation can be less than the cost of a bilinear pairing computation. Decryption is the term used to describe the process of deciphering the first ciphertext (or).

When working with encrypted ciphertext, decryption is referred to as Dec(Re), which stands for the inverse of encryption. The greatest possible value of |S| or l is denoted by the letter M. Calculating an exponentiation is straightforward, and hence disregarding the cost of the hash operation is only a minor drawback in our technique. In Table II, the costs of the algorithms are the same regardless of whether the specified security parameter is strong or weak. When it comes to public key searchable encryption systems, the efficiency of our method is virtually as good as the efficiency of the competition.

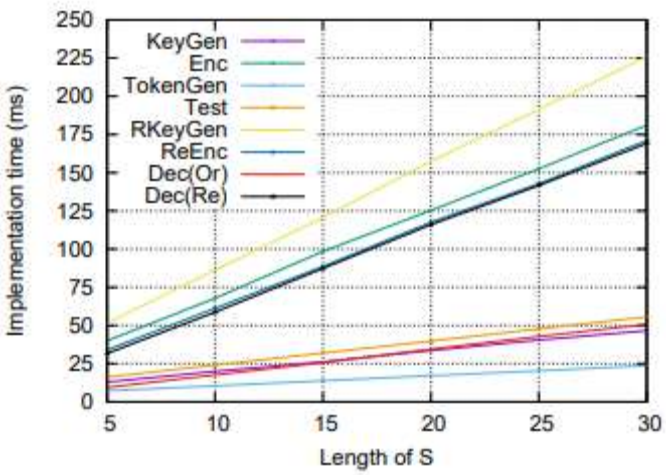

Fig.1.Implementation Time.

Even though our plan will be more expensive during the test time, the CPAB-KS plan will be more expensive over the entire test period. The ability to share data with others is an additional degree of calculation that should be considered. Our proposed KeyGen, Enc, and TokenGen prices are essentially identical to those of the PRE-KS system; however, ours is substantially less expensive when it comes to the costs of computation for the KeyGen, Enc, and TokenGen functions. Using our technique, which is more expensive than KPAB893 PRE-KS, results in a calculation cost for T est, ReEnc, Dec(Or), and Dec(Rec) that is approximately the same order of magnitude as KPAB893 PRE-KS. The KPAB-

PRE-KS scheme generates a single input for the bilinear map, which eliminates the need for characteristics to be multiplied in order to be included as a component of an input. Despite the fact that being a member of the PKG is required in the KPAB-PRE-KS system, as far as we are concerned, the absence of packages that cut computing costs has had no impact on our approach. Our solution necessitates the calculation of the PKG re-encryption key to be conducted without any interaction with the delegator. By eliminating PKG, it would have a positive impact on the overall PKG load.

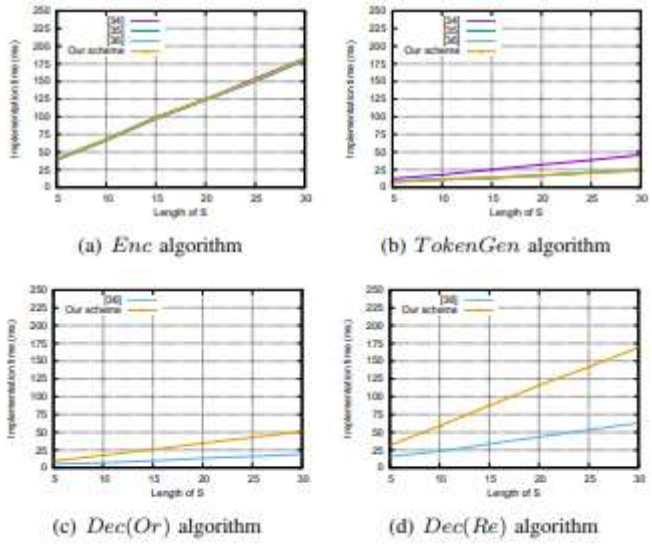

Fig.2. Implementation Time Comparison

C. Implementation

The Go-based Golang PBC package was created in order to make use of the open source Golang PBC package that is already available. This Intel i5-8250U processor, which is part of the 6th generation, is clocked at 1.6GHz and comes with 8GB of RAM, as well as the newest hardware technology. It was discovered that Y2 = X3 + X is the sole elliptic curve with the equation Y2 = X3 + X, and that the group order for this curve is 160 bits. Various parts of the experiment were repeated 20 times, with each repetition beginning at a different step of the operation, in order to calculate an exact average execution time. The value is set to 1000 in this case. Set the value of S to 5 in order to make the KenGen algorithm available. Assume you have a definition for row l = 5, with the limitation that only certain users are able to access it (this is known as an access policy), and that the mapping for each row I in the range 1 I l becomes (i). The runtime details are summarised in Table III. The fact that the stages were changed from 5 to 30 is noteworthy, but it is the inclusion of step 20, which was previously absent, that is the most significant difference. Results from Table III and Figure 1 are compared to see whether there is a difference in the amount of time required to execute each algorithm. According to our theoretical research, the time it takes for an algorithm to execute is approximately linear to the size of S. Despite the fact that the re-encryption functionality looks to be ineffective, the Enc technique consumes 80 percent of the time spent in RKeyGen. The delegator has the ability to re-run the algorithm to generate a ciphertext that contains the amended policy and keyword in the event that the method's parameters are altered. In addition to this, re-running Enc will reveal that the recommended proxy re-encryption technique does not function properly. Recomputation The initial step of key creation allows the delegator to recomputation the ciphertext several times, hence reducing the total cost of the operation for the delegator. It is also advantageous to delegate using this technique because the delegator does not have to perform any additional steps such as retrieving data from the cloud server, decrypting that data in order to recover the underlying plaintext, and re-encrypting the plaintext with a new policy and keyword after the delegator has completed these steps. Data issues arising from the use of the cloud to obtain data are increasingly becoming apparent. The mechanisms that have been proposed previously for implementing digital signature will be reviewed as well, as all of these ways may be utilised in the public key environment and regulate user identity. While conducting our analysis, we did not compare the implementation time to normal scheme work implementation timings, which would have been inappropriate. As an example of how algorithms like this function on the user's side of the equation, we used the

Enc, TokenGen, Dec(Or), and Dec(Re) algorithms. We can observe in Fig 2(a) that our compute cost is exactly the same as the compute costs of the other systems. Our TokenGen approach has an efficiency that is substantially comparable to that of [35] and [36], and it outperforms scheme [34] by almost the same margin. The computations required by our proposed technique are significantly bigger than those required by [36] (as illustrated in Figures 3(a) and 3(b)). By doing away with the obligation to interact with the PKG, we have alleviated some of the strain placed on the PKG in subsection V-B of this document.

5. CONCLUSION

The new paradigm established by this paper will improve search and data sharing for the CIPAB-KSDS system, according to the authors. The Random oracle of the CCA safety model, when applied to a specific CPAB-KSDS, performs as promised in our prototype. The proposition was rejected outright. Using this experiment, it was demonstrated that the technique is accurate and advantageous for determining whether work and property outcomes are equivalent. This article serves as an introduction for those who wish to pursue the topic further. a query that receives no response and a positive response Using the keyword search tool and encrypting data sharing are both techniques for improving on a function that was previously available to users. You'll need to be in the sharing phase if you don't have the PKG. In addition, we offer It is a complicated and thought-provoking project, which we can also supply. CPAB-KSDS was created without the use of oracles, and there were no random oracles used in the creation of the system. Implement a new framework for looking for sentences that are written in an expressive manner.

REFERANCE:

- Secure keyword search and data sharing mechanism for cloud computing Chunpeng Ge, Willy Susilo, Zhe Liu, Jinyue Xia, Pawel Szalachowski, Fang Liming.
- Ibtihal, Mouhib, and Hassan Naanani, 2020,Homomorphic encryption as a service for outsourced images in a mobile cloud computing environment, In Cryptography: Breakthroughs in Science andPractice, pp. 316-330. Global IGI.
- Buyyya, R., Yeo, C.S., Venugopal, S., Broberg, J. And Brandic, I, 2009,Cloud computing and emerging IT platforms: vision, hype, and fact to offer computing as the 5th utility, Future Generation of Computer Systems, 25(6), pp. 599-616.
- Aljawarneh, S., 2011,Web innovation safety approach for e-learning applications, Network Security, p. 12-15.
- Organisation for Economic Co-operation and Development, 2002,OECD guidelines on the protection of privacy and transborder flows of personal data, OECD Publishing.
- Alnajrani, H.M., Norman, A.A. and Ahmed, B.H., 2020,Privacy and data protection in mobile cloud computing: A systematic mapping study, Plos one, 15(6), p.e0234312.
- M. Ali et al., June 2017, SeDaSC: Secure Data Sharing in Clouds, in IEEE Systems Journal, vol. 11, no. 2, pp. 395-404, doi: 10.1109/JSYST.2014.2379646.
- Eltayieb, N., Elhabob, R., Hassan, A. and Li, F., 2020,A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud, Journal of Systems Architecture, 102, p.101653.
- Sinha, D., Datta, S. and Das, A.K., 2020,Secure Data Sharing for Cloud-Based Services in Hierarchical Multi-group Scenario,in Advances in Computational Intelligence, pp. 229-244, Springer, Singapore.
- Sahai and B. Waters, “Fuzzy identity-based encryption,” in Annual 981 International Conference on the Theory and Applications of Crypto982 graphic Techniques, pp. 457–473, Springer, 2005. 983

- V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp984 tion for fine-grained access control of encrypted data," in Proceedings 985 of the 13th ACM conference on Computer and communications security, 986 pp. 89–98, Acm, 2006. 987
- J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute988 based encryption," in Security and Privacy, 2007. SP'07. IEEE Sympo989 sium on, pp. 321–334, IEEE, 2007. 990
- Waters, "Ciphertext-policy attribute-based encryption: An expressive, 991 efficient, and provably secure realization," in International Workshop on 992 Public Key Cryptography, pp. 53–70, Springer, 2011. 993.