IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# PRIVACY PRESERVING KEYWORD SEARCH SCHEME OVER ENCRYPTED CLOUD DATA AN EXTENSIVE ANALYSIS

[1]Maguluri Akhil Chowdary, [2]Shashirekha H

[1]Student, [2]Assistant Professor

[1]Department of Computer Science and Engineering ,

[1]VTU CPGS Mysuru,Ongole , India

***Abstract:*** Cloud storage offerings have emerge as increasingly more popular. In truth cloud does now not aid solely one or two consumer rather they helps hundreds of thousands of customers and as a result privateness problems of information is incurred. Because of the significance of privacy, many cloud storage encryption schemes have been proposed to guard facts from these who do now not have access. To tackle this problem, impenetrable and privateness maintaining key-word search over massive scale cloud statistics is proposed and broadly developed All such schemes assumed that cloud storage companies are secure and can't be hacked. For that we are going to strengthen invulnerable search protocol. We additionally analyze the privateness and effectivity of proposed schemes in detail. The scan outcomes exhibit that our proposed schemes are efficient

***Index Terms*** **- Privacy, Keyword Search,Encryption, Cloud Data.**

## I. INTRODUCTION

Cloud computing as the definition given by National Institute of Standards and Technology (NIST), is "an enabling ubiquitous model, provides us network access based on demand and offers a convenient aid of collection of configurable resources like servers, networks and storage applications, various services, which has the ability to be quickly provisioned and released with minimum effort from service provider interface or minimal management effort." The three common cloud service models offered by cloud is software as a service (SaaS), Infrastructure as a service (IaaS) and Platform as a service (PaaS). Out of this, Cloud storage is the main important service offered by cloud computing, it helps users to move their data in to the cloud from local storage systems. It is an easy and cost effective way to store and manage the data. Drop box and Google Docs is an example of cloud storage system and it now becomes the essential feature in storage offerings. Among numerous services provided by cloud computing, cloud storage service, such as Apple's iCloud, Microsoft's Azure and Amazon's S3, can offer a more flexible and easy way to share data over the Internet.

Keyword search is one of the critical and most familiar statistics operations. Many present latest schemes are keyword-based search which include single key-word and multi-keywords etc. Boolean key-word search scheme solves the hassle of supporting environment friendly ranked key-word search. By doing this high-quality utilization of remotely saved encrypted facts is done in Cloud Computing. It enhances machine usability by means of returning the matching files. These schemes enable facts customers to retrieve involved archives and return associated archives in the encrypted form. To make sure that the consumer can function a search over the encrypted information except revealing the records to the server. The cryptographic primitive that affords this characteristic is broadly recognized as searchable encryption. Searchable encryption permits the customers to generate a search token from the searched key-word in such a way that the cloud server can retrieve the encrypted contents containing the searched keyword.

Firstly, outsourcing facts to cloud server implies that facts is out manipulate of users. This can also purpose customers hesitation given that the outsourced facts typically comprise treasured and touchy information. Secondly, records sharing is regularly carried out in an open and adverse environment, and cloud server would emerge as a goal of attacks. Even worse, cloud server itself might also expose users' statistics for unlawful profit. Thirdly, information sharing is now not static. That is, when a user's authorization receives expired, he/she must no longer possess the privilege of getting access to the beforehand and because of this shared data. Therefore, whilst outsourcing statistics to cloud server, customers

additionally desire to manage get entry to to these facts such that solely these presently approved customers can share the outsourced data.A na\tural answer to overcome the aforementioned hassle is to use cryptographically enforced get entry to manage such as identity-based encryption (IBE). Furthermore, to overcome the above protection threats, such sort of identity-based get admission to manipulate positioned on the shared records need to meet the following safety goals:Data confidentiality,Backward secrecy,Forward secrecy.we suggest the scheme of provable records Efficient Privacy Preserving Integrity Checking Model for Cloud Data Storage Security. The particular hassle addressed in this paper is how to assemble a necessary identity-based cryptographically device to reap the above safety goals.

## II. PROPOSED SYSTEM

Techniques used in preceding deniable encryption schemes, we construct two encryption environments at the identical time, a whole lot like the notion proposed in .We construct our scheme with more than one dimensions whilst claiming there is solely one dimension. This strategy gets rid of apparent redundant components in. We follow this notion to an current ABE scheme through changing top order organizations with composite order groups. Since the base ABE scheme can encrypt one block every time, our deniable CPABE is honestly a blockwise deniable encryption scheme. Though the bilinear operation for the composite order team is slower than the top order group, there are some methods that can convert an encryption scheme from composite order businesses to high order organizations for higher computational performance.

It looks that the idea of revocable identity-based encryption (RIBE) would possibly be a promising method that fulfills the aforementioned safety necessities for information sharing.

RIBE points a mechanism that allows a sender to append the cutting-edge time duration to the ciphertext such that the receiver can decrypt the ciphertext solely below the situation that he/she is no longer revoked at that time period.

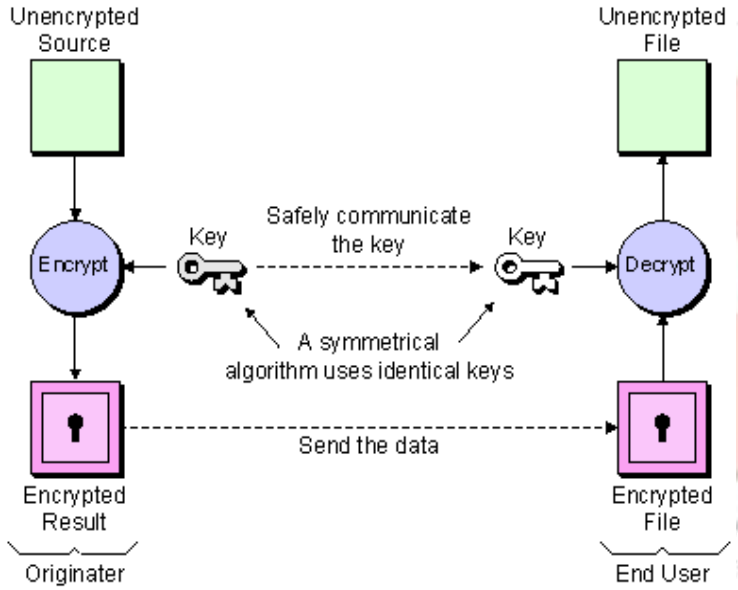


Figure1:block diagram

## III. LITERATURE SURVEY

*Table 1: summary of important investigation*

| S. No | Year of Published | Author Name | Title | Methodology | Results |
|---|---|---|---|---|---|
| 1 | 2018 IEEE | Prasanthi Sreekumari | Privacy preserving keyword search scheme over encrypted cloud data an extensive analysis | Searchable encryption scheme, Requirements for protecting privacy, Architecture of PRMSM, Overview of VP search and architecture of PSS over multiple cloud. | Verifiability, Efficiency and Data privacy |
| 2 | 2018 IEEE | Runze Ji ; Nankun Mu ; Xiaofeng Liao | A Novel Privacy-Preserving Data Integrity Verification by Partial Delegation | a new storage model, there are known security and privacy issues in migrating data to the cloud. | cost of basic cryptographic and analyzing the experiment show, the proposed schemes are highly efficient and practical |
| 3 | 2018 IJC | Geeta C Ma *, Raghavendra Sb , Rajkumar Buyyac , Venugopal K Rd , S S Iyengare , L M Patnaik | Data Auditing and Security in Cloud Computing: Issues, Challenges and Future Directions | Cloud information repository is involved with issues of information integrity, data security and information access by unapproved users. | Directions for future research in data auditing and security have been discussed. |
| 4 | 2017 IEEE | Zhangjie Fu, Fengxio Huang, Kui Ren, Jain Weng & cong wang | Privacy preserving smart semantic search based on conceptual graphs over encrypted outsourced data. | Searchable encryption, smart semantic search, conceptual graphs. | Privacy and efficiency |
| 5 | 2017 | Baoyuan Kang, Jiaqiang Wang, Dongyang Shao | Attack on Privacy-Preserving Public Auditing Schemes for Cloud Storage | security analysis of these schemes | Schemes are vulnerable to an attack from the malicious cloud server who modifies the data blocksandsucceeds in forging proof information for dataintegrity check |

| | | | | | |
|---|---|---|---|---|---|
| 6 | 2016 IJARIIE | Vanita Gadekar, Baisa Gunjal | Privacy preserving ranked multi keyword search of multiple data owners in cloud computing | Multi keyword search<br><br>Boolean keyword search, | Hides user's identification that is having information on cloud, to degree up the protection constraints.<br><br>Provides backup facility in which final modified replica of information must preserve. |
| 7 | | Wei Zhang, Jie Wu, Yaping Lin | Secure and privacy preserving keyword search over the large scale cloud data | Searchable encryption, Ranked keyword search, Fuzzy keyword search, Conjunctive keyword search, Similarity keyword search, Attribute based keyword search. | Secure & privateness keeping key-word search over giant scale cloud data. |

## IV. CONCLUSION

Cloud computing brings terrific remedy for people. We advocate two greater impenetrable and surroundings pleasant schemes to clear up the trouble of privacy-preserving wise semantic search especially based totally on conceptual graphs over encrypted outsourced data Particularly, it flawlessly fits the prolonged desire of sharing data over the Internet. To assemble a low priced and impenetrable information sharing computer in cloud computing, we proposed a questioning recognised as RS-IBE, which helps identification revocation and cipher textual content exchange at the same time as such that a revoked client is averted from getting get admission to to in the past shared data, as well as due to this truth shared data. Furthermore, a concrete improvement of RS-IBE is presented. The proposed RS-IBE scheme is proved adaptive-secure in the giant model, underneath the decisional ℓ-DBHE assumption. The distinction consequences divulge that our scheme has advantages in phrases of effectivity and functionality, and as a end result is more plausible for sensible applications. We furnish the feasible reply for keeping privateness for multi-data owners.

## *V.* References


1. Understanding trust and privacy of Big data in social Networks -A brief Review Shashi Rekha IEEE 2014
2. Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption Jianghong Wei, Wenfen Liu, Xuexian Hu IEEE 2018
3. A Novel Privacy-Preserving Data Integrity Verification by Partial Delegation Runze Ji ; Nankun Mu ; Xiaofeng Liao IEEE 2018
4. Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption Ms.Kiruba J, N. Angala Eswari , M. Kavipraba , A. Mugilarasi , G. Nithya IEEE 2018
5. SEPDP: Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage Sanjeet Kumar Nayak ; Somanath Tripathy IEEE 2018
6. A Survey Paper On Efficient Privacy Preserving and Secure Data Integrity Protection In Regenerating Coding Based Public Cloud Storage" Monika B Thakare , Prof. N.M.Dhande IRJET 2018
7. Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE 2018
8. Data Auditing and Security in Cloud Computing: Issues, Challenges and Future Directions Geeta C Ma *, Raghavendra Sb , Rajkumar Buyyac , Venugopal K Rd , S S Iyengare , L M Patnaik IJC 2018
9. Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption Swapnil Deshmukh, Sourabh Dhivare, Prof.Mr. Harshad Dagade IJSER 2018Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption Kishore Babu V, Amutha IJSDR 2018
10. Privacy preserving model: a new scheme for auditing cloud stakeholders Abdul Razaque & Syed S. Rizvi 2017
11. Attack on Privacy-Preserving Public Auditing Schemes for Cloud Storage Baoyuan Kang, Jiaqiang Wang, and Dongyang Shao 2017
12. Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage Jyoti R Bolannavar IJSER 2016.