© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

A Novel Approach for Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

V Ramana Chintalapudi[1], Mohammed Alisha[2], Dr. D. Mohan Reddy[3]

[1]PG Scholar, Department of Computer Science and Engineering, Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram, East Godavari District, Andhra Pradesh, India

[2]Associate Professor & Head of the Department, Computer Science and Engineering, Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram, East Godavari District, Andhra Pradesh, India

[3]Professor & Principal, Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram, East Godavari District, Andhra Pradesh, India

ABSTRACT

Unique Cloud computing is another motivation innovation which productively bolster the customer arranged administrations. Presently in nowadays there are figures of uses which eat up the cloud storage benefit for keep and get back data. In such express the information owner administration and protection conservation cryptographic procedures are make utilization of oftentimes. In our examination, the watchword seek over encoded information with differential right is tended to. We give a new substructure to secure outsourcing and sharing of encrypted information on cross hybrid cloud. The system is full-highlighted: i) it empowers perceived clients to perform watchword construct seek straightforwardly in light of encrypted information without having a similar private key; ii) it gives two-layered access control to accomplish fine-grained sharing of encoded information. The security investigation demonstrates that the proposed non specific erection fulfills the necessities of message protection and key words security.

Keywords: Cloud computing, key word search, cryptographic, hybrid cloud.

I. INTRODUCTION

Cloud storage outsourcing has turned into a famous application for endeavours and associations to decrease the weight of keeping up enormous information lately. In any case, in all actuality end clients may not by any stretch of the imagination believe the cloud storage servers and may want to encode their information before transferring them to the cloud server with a specific end goal to ensure the information protection. This more often than not makes the information usage more troublesome than the conventional stockpiling where information is kept without encryption. One of the common arrangements is the accessible encryption which enables the client to recover the encoded records that contain the client determined watchwords, where given the key words trapdoor, the server can discover the information required by the client without decoding. The PHRs are encrypted keeping in mind the end goal to agree to security controls like HIPAA. Note that the setting we are thinking about backings private information sharing among various information suppliers and different information clients. In this manner, SE plots in the private-key setting, which accepts that a solitary client who seeks and recovers his/her own particular information are not appropriate. In a PEKS framework, utilizing the

collector's open key, the sender joins some encoded watchwords (alluded to as PEKS ciphertext) with the encrypted information. The collector at that point sends the trapdoor of a to-be-scanned watchword to the server for information seeking. Given the trapdoor and the PEKS ciphertext, the server can test whether the watchword hidden the PEKS ciphertext is equivalent to the one chose by the collector. Assuming this is the case, the server sends the coordinating encrypted information to the beneficiary. PEKS plans experience the ill effects of an innate weakness with respect to the trapdoor watchword security, to be specific inside Keyword Guessing Attack (KGA).

The reason prompting such security defencelessness is, to the point that any individual who knows recipient's open key can create the PEKS ciphertext of self-assertive key words himself. In particular, given a trapdoor, the ill-disposed server can pick speculating key words from the watchword space and afterward utilize the key words to produce a PEKS ciphertext. The server at that point can test whether the speculating key words is the one fundamental the trapdoor. This speculating then-testing technique can be rehashed until the point when the right watchword is found. Such a speculating assault has additionally been considered in numerous secret key based frameworks.

II. Overview of Cloud

Cloud computing gives us a methods by which we can get to the applications as utilities, over the Internet. It enables us to make, design, and tweak applications on the web. With Cloud processing clients can get to database assets by means of the web from anyplace for whatever length of time that they require without stressing over any upkeep or administration of genuine assets.

Cloud computing alludes to controlling, designing and getting to the applications on the web. It offers online information stockpiling, foundation and application. It is both a mix of programming and equipment based processing asset conveyed as a system benefit.

2.1 Basic ideas: There are sure administrations and models working behind the scene making the cloud computing achievable and available to end clients. Following are the working models for cloud computing: (I) Deployment Models (ii) Service Models.

2.1.1 Deployment Models: Arrangement Models characterize the sort of access to the cloud, i.e., how the cloud is found? Cloud can have the four kinds of access. (I) Public (ii) Private (iii) Hybrid and (iv) Community.

Figure: 1 Four types of cloud computing

The above Fig. 1 shows the types of cloud computing. These types are detailed as follows.

Private Cloud: The Private Cloud enables framework and administrations to be available inside an association. It offers expanded security due to its private nature.

Open Cloud: people in general Cloud permits and administrations to be effectively available to the overall population. Open cloud might be less secure as a result of its transparency, e.g., email.

Community Cloud: The Community Cloud enables frameworks and administrations to be an available by gathering of associations. Hybrid Cloud: The Hybrid Cloud is blend of open and private cloud while the non-basic exercises are performed utilizing open cloud.

2.1.2 Service Models: Service Models are the reference models on which the Cloud Computing is based. These can be arranged into three essential administration models as listed.(i) Infrastructure as a Service(IaaS) (ii) Platform as a Service(PaaS) (iii) Software as a Service(Saas).

Infrastructure as a Service (IaaS): It is the conveyance of innovation foundation as an on request versatile administration. IaaS gives access to essential assets, for example, physical machines, virtual machines, virtual capacity, and so on.

Platform as an administration (PaaS): It gives the runtime condition to applications, improvement and arrangement apparatuses, and so forth.

PaaS gives the majority of the offices required to help the total life cycle of building and conveying web applications and administrations altogether from the Internet. Ordinarily applications must be created in light of specific stage Multi occupant situations

Highly versatile multi level design Software as a Service (SaaS): It gives product administrations to the end client. Electronic email and Google Documents are maybe the best-known case of SaaS. End client gets the entrance to utilize the product utility yet he has no rights to change or to alter it. Programming isn't introduced on end client PC it is designed in cloud. End client needs to pay for the administration as per their necessities.

III. Challenges of Searchable Encryption

The first objective of accessible encryption is to give security safeguarding watchword quests of encrypted information against a middle passage, for example, a mail server or a system switch, A. B. Lewko et al. involves a message trade process between the sender and the collector. The accessible encryption conspires that empowers watchword look over information encrypted with various keys. The plan is functional and was intended to be incorporated into another framework for ensuring information privacy in customer server applications against assaults on the server. We examine about the engineering and security necessities for accessible encryption plot.

3.1 Searchable encryption Architecture: Searchable encryption (SE) empowers the clients to produce a hunt token from the sought key words in such way that given a token, the cloud server can recover the encrypted substance containing the looked watchword. Essentially, the pursuit token speaks to an encoded inquiry over the encrypted information and can be produced just by clients with the proper mystery key. Fig. 2 demonstrates the essential engineering and working standard of an accessible encryption plot. The engineering includes for the most part four elements: information owner, information client, cloud specialist co-op and key generator. A concise depiction of the substances and their operations are given underneath.

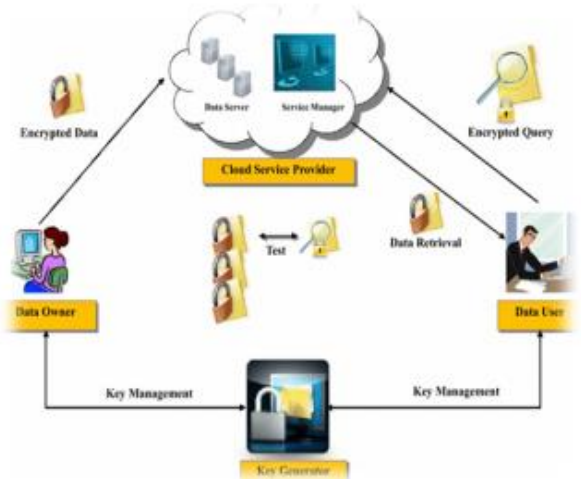

Figure: 2 Architecture of a searchable encryption scheme.

· **Data owner**: The information owner is the element which produces and encodes the information and transfers them to the cloud server. It can be either an association or a person. To utilize the administration, the information owner utilizes its application which comprises of an information processor for transferring new substance to the cloud. It encodes the information and metadata with a cryptographic plan that empowers looking ability.

·**Data client**: This element is additionally an endorser of the cloud storage which sends encoded questions to the cloud specialist organization to look for particular encrypted information. There might be more than one information client in the framework and in some situation, the information owner and the information client may be a similar substance.

·**Cloud specialist co-op:** This substance gives the information stockpiling and recovery administration to the endorsers. The cloud specialist co-op comprises of cloud information server and cloud benefit chief. The principal element is utilized to store the outsourced encrypted information while the last one

is utilized for information administration in the cloud. After accepting the encoded look inquiries from the information client, the cloud specialist organization tests on the encrypted questions and encoded metadata in the cloud storage. The encrypted information that fulfils the hunt criteria is recovered and sent back to the information endless supply of the test. The cloud specialist co-op ought not to take in any data from the operation.

• **Key generator**: This substance is thought to be a trusted outsider who is in charge of the age and administration of the encryption/unscrambling keys. Client particular keys are created and disseminated amid the setup of the framework.

3.2 Searchable Encryption Security Requirements All in all, the accompanying prerequisites ought to be fulfilled while building an accessible encryption plot.

• **Retrieved information:** Server ought not to have the capacity to recognize records and decide look substance.

• **Search inquiry:** Server ought not to get the hang of anything about the watchword being hunt down. Given a token, the server can recover nothing other than pointers to the encrypted substance that contains the key words.

• **Query age:** Server ought not to have the capacity to produce a coded question. The inquiry can be created by just those clients with the applicable mystery key.

• **Search question result:** Server ought not to get the hang of anything about the substance of the hunt result.

• **Access designs:** Server ought not to find out about the arrangements and recurrence of records got to by the client.

• **Query designs:** Server ought not to learn whether two tokens were proposed for the same inquiry.

IV. Related Work

In this section, we present a brief summary of related works dealing with the searchable encryption schemes. Searchable encryption scheme can be designed in either public cloud or private cloud.

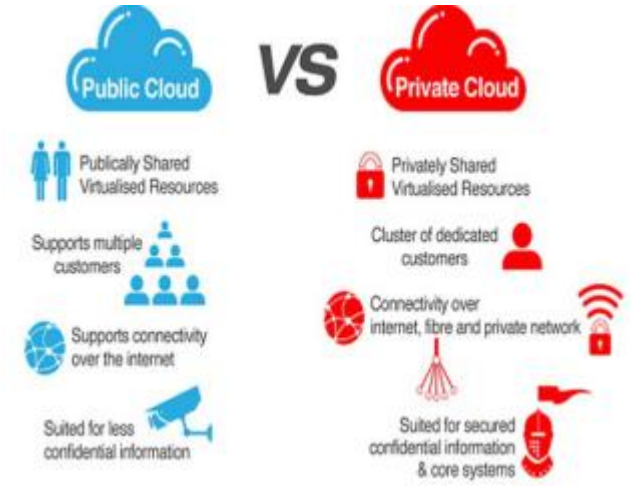

Figure: 3 Basic concept of Public Cloud vs. Private Cloud

The main accessible encryption plot out in the open cloud was proposed by Jin Li et al. Open cloud benefits on assets that are shared between numerous clients, oversaw off-premises and adaptable homogeneous foundation. People in general cloud storage is straightforward however inquisitive and the way that the two correspondence joins (i.e. one is between put stock in private cloud and open cloud storage, and the other is amongst client and open cloud storage) are uncertain in classification. ii) An inquisitive client, who can acquire his individual private key and offer his validation with different clients. Next we think about private cloud was proposed by E. Goh et al. We accept the private cloud is completely trusted and consider general society cloud storage semi-trusted, all the more exactly, it will take after our proposed convention yet endeavour to discover however much private data as could reasonably be expected in light of its ownership. Be that as it may, private cloud was controlled and heterogeneous framework. At long last the half and half cloud we outdo both.

V. Proposed Solution

In our examination means to plan and build up a protection saving information stockpiling and recovery framework in cloud computing. The extensions include the utilization of accessible encryption calculations to scan for particular watchwords inside an encrypted substance, i.e.,

without requiring the client to download the database and decode its substance before looking can be performed utilizing Hybrid cloud. In this paper, we consider a novel key words seek engineering in crossover cloud that is, a trusted private cloud and public cloud are accepted in our framework. The usage of the half and half cloud computing framework empowers the clients to seek effectively, as well as receives the rewards of approaching administrations and applications from cloud specialist organizations. This enables us to grow our web nearness and still keep up some level of independence and security. Under the mixture design, we give a novel system to outsourcing and sharing accessible encrypted information. In our exploration to recover all the encrypted PHRs containing a key words, say "Diabetes", a client sends a "trapdoor" related with a pursuit question on the watchword "Diabetes" to the cloud specialist organization, which chooses all the encoded PHRs containing the key words "Diabetes" and returns them to the client while without taking in the basic PHRs. Notwithstanding, the arrangement and additionally other existing PEKS plans which enhance just help equity questions. In the above cloud-based medicinal services framework, to discover the connection amongst diabetes and age or weight, a restorative scientist may issue an inquiry question with an entrance structure (i.e., predicate) ("Illness = Diabetes" AND ("Age = 30" OR "Weight = 150-200")).

VI. Conclusion

In the paper, we exhibit a novel system for information outsourcing and sharing on the half and half cloud computing. It comprises of a confided in private cloud and public cloud storage. In the structure, the capacity server can perform look on encrypted information without taking in the fundamental plaintexts in the public key setting, X. Zhou proposed a cryptographic crude called open key encryption with key words seek (PEKS). From that point forward, thinking about various prerequisites practically speaking, e.g., correspondence overhead, looking criteria and security upgrade, different sorts of accessible encryption frameworks have been advanced. In any case, there exist just a couple of open key accessible encryption frameworks that help expressive watchword look strategies, and they are altogether worked from the wasteful composite-arrange gatherings. In this paper, we concentrated on the outline and investigation of open key accessible encryption frameworks in the prime-arrange bunches that can be utilized to look through different key words in expressive seeking equations.

VII. REFERENCES

[1]. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in 2013 IEEE Symposium on Security and Privacy, Berkeley, California, USA, May 14-17, 2000. IEEE Computer Society, 2014, pp. 44–55.

[2]. J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Computational Science and Its Applications - ICCSA 2014, International Conference, Perugia, Italy, June 30 - July 3, 2015, Proceedings, Part I, ser. Lecture Notes in Computer Science, vol. 5072. Springer, 2014, pp. 1249–1259.

[3]. M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in 2013 International Conference on cloud Computing Systems, ICDCS 2013, Minneapolis, Minnesota, USA, June 20-24, 2014. IEEE Computer Society, 2014, pp. 383–392.

[4]. A. B. Lewko, A. Sahai, and B. Waters, "Revocation systems with very small private keys," in 31st IEEE Symposium on Security and Privacy, S&P 2010, 16-19 May 2010, Berleley/Oakland, California, USA. IEEE Computer Society, 2015, pp. 273–285.

[5]. W. Ogata and K. Kurosawa, "Oblivious keyword search," J. Complexity, vol. 20, no. 2-3, pp. 356–371,2015.

[6]. Jingwei Li, Chunfu Jia, Jin Li, and Zheli Liu, "A Novel Framework for Outsourcing and Sharing Searchable Encrypted Data on Hybrid Cloud" 2014 Fourth International Conference on Intelligent Networking and Collaborative Systems.

[7]. Md Iftekhar Salam1, Wei-Chuen Yau2, Ji-Jian Chin2, Swee-Huay Heng3, Huo-Chong Ling4, Raphael C-W Phan2," Implementation of searchable symmetric encryption for privacy-preserving keyword search on cloud storage", Salam et al. Hum. Cent. Comput. Inf. Sci. (2015).

[8]. O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," J. ACM, vol. 43, no. 3, pp. 431–473, 2015.

[9]. E. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol. 2010, p. 216, 2013.

[10]. Jin Li, Xiaofeng Chen,"efficient multi-user keyword search over encrypted data in cloud computing" Computing and Informatics,2013.

[11]. J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, "Expressive search on encrypted data," in 8th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '13, Hangzhou, China - May 08 - 10, 2013. ACM, 2013, pp. 243–252.

[12]. Mahesh Kallahalla, Erik Riedel, Ram Swaminathan, Qian Wang, and Kevin Fu. Plutus: Scalable secure file sharing on untrusted storage. In Proc. of USENIX FAST, 2003.

[13]. Eu-Jin Goh, Hovav Shacham, Nagendra Modadugu, and Dan Boneh. Sirius: Securing remote untrusted storage. In Proc. of NDSS, 2003.

[14]. Tatsuaki Okamoto and Katsuyuki Takashima. Hierarchical predicate encryption for inner-products. In Advances in Cryptology–ASIACRYPT 2009, pages 214–231. 2009.

[15]. Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. Privacy- preserving multi-keyword ranked search over encrypted cloud data. Parallel and Distributed Systems, IEEE Transactions on, 25(1):222–233, 2014.

ABOUT AUTHORS:

V.RAMANA CHINTALAPUDI is currently pursuing his M.Tech Computer Science & Engineering at Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram.

MOHAMMED ALISHA is currently working as a Associate Professor and Heading the Department of Computer Science and Engineering at Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram. He is a Post Graduate in Computer Science and Engineering and had 12 years of Experience. His Research interests include Spatial Data Mining, Web Designing, Java Programming, Computer Networks and Data Warehousing.

Dr. D. MOHAN REDDY received the B.Tech. Degree from Jawaharlal Nehru Technological University, Hyderabad, India and he received the M.E from Anna University, Chennai and Ph.D from Sri Venkateswara University, Tirupati, India. Presently he is working as a Professor & Principal in Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram. His research areas of interests are power electronic converters & Intelligence Systems .