WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Advanced Model for Keyword Search of Cloud Computing with Data Security

***K Ramesh Babu*[*1], *D. Ram Mohan Reddy*[*2], *K. Srinivasa Rao*[*3], *Mamatha. N*[*4]**

[1]Research Scholar, Dept of CSE, GVR&S CET, Guntur
[2]Associate. Professor, Dept of CSE, Newton's Institute of Engineering, Macherla
[3]Research Scholar, Dept of CSE, NRIIT, Guntur.
[4]Research Scholar, Dept of CSE, Newton's Institute of Engineering, Macherla
DOI: https://doi.org/10.55248/gengpi.4.1223.0134

A B S T R A C T

Cloud computing becoming more and more widespread, safer and more effective ways to locate and retrieve data from cloud storage are needed. this research presents a sophisticated keyword-searching strategy designed to protect data in cloud computing settings. uses sophisticated encryption methods like symmetric-key, homomorphic, and attribute-based encryption to guarantee data security and secrecy. Additionally, in order to shorten search times and increase search efficiency, this work presents an optimized indexing method based on the binary search algorithm. Additionally, in order to provide quick calculation among numerous parties while maintaining the privacy of private information, our model uses a secure multi-party computation approach. This work shows that the suggested model provides good accuracy and efficiency while preserving data security using a benchmark data set. The suggested paradigm can be applied to a number of fields where sensitive data needs to be safely kept and accessed, including e-commerce, healthcare, and finance. The suggested methodology offers cloud computing environments an effective and safe way to search for keywords.

Keywords: cloud computing, security, data security, keyword search etc.,

1. Introduction

The subversive technology of cloud computing is changing the way IT hardware and software are developed and gained. Cloud computing, a new paradigm in computing, offers numerous benefits such as cost savings, rapid deployment, simplified resource management, and ease of use. it can help businesses of all sizes become more innovative and collaborative.Not withstanding the many advantages of cloud computing, people and businesses are hesitant to transfer sensitive data such as emails, private medical records, and government-only documents to the cloud due to privacy concerns. This is due to the fact that the owners of the relevant sensitive data no longer have direct control over them once they are outsourced to a distant cloud. Cloud service providers (CSPs) would guarantee the security of owners' data by using virtualization and other techniques.The main contributions of this paper are listed as follows.It will define a multi-owner model for privacy p-reserving keyword search over encrypted cloud data.Proposing an efficient data user authentication protocol, which not only prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation systematically construct a novel secure search protocol, which not only enables the cloud server to perform secure ranked keyword search with- out knowing the actual data of both keywords and trapdoors, but also allows data owners to encrypt

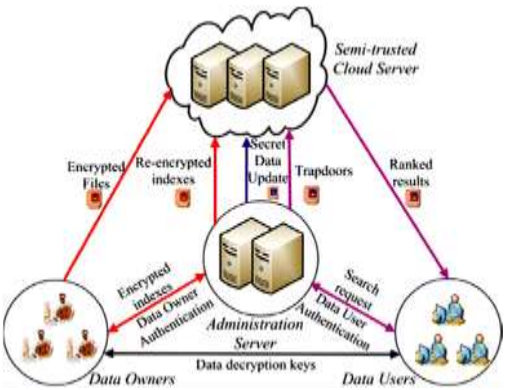

Fig.1: Architecture of privacy preserving keyword searchinga multi owner and multi-user cloud model

Keywords with self-chosen keys and allows authenticated data users to query without knowing these keys.Also proposed an Additive Order and Privacy Preserving Function family(AOPPF) which allows data owners to protect the privacy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurately.Conduct extensive experiments on real-world datasets to confirm the efficacy and efficiency of our proposed schemes

System Model: In our multi-owner and multi-user cloud computing model, four entities are involved, as illustrated in Fig.1, they are data owners, the cloud server, Administration server and data users. Data owners have a collection of files. To enable efficient search operations on these files which will be encrypted, data owners first build a secure searchable index on the keyword set extracted from, and then they submit to the administration server. Finally, data owners encrypt their files and outsource the corresponding encrypted files to the cloud server. Upon receiving, the administration server re-encrypts for the authenticated data owners and out sources the re-encrypted index to the cloud server. Once a data user wants to search t keywords over these encrypted files stored on the cloud server, the first computes the corresponding trapdoors and submits them to the administration server. Once the data user is authenticated by the administration server, the administration server will further re-encrypt the trapdoors and submit them to the cloud server. Upon receiving the trapdoor, the cloud server searches the encrypted index of each data owner and returns the corresponding set of encrypted files.

To improve the file retrieval accuracy and save communication cost, a data user would tell the cloud server a parameter k and cloud server would return the top-k relevant files to the data user.

Overview is it's giving an example to illustrate the main idea of the user authentication protocol (the detailed protocol is elaborated in the following subsections). Assume Mr. Rama wants to be authenticated by the administration server, so he starts a conversation with the server. The server then authenticates the contents of the conversation. If the contents are authenticated, both Mr Rama and the server will generate the initial secret key according to the conversation contents. After the initialization, to be authenticated successfully, Mr Rama has to provide the historical data of their conversations. If the authentication is successful, both Mr Rama and the administration server will change their secret keys according the contents of the conversation. In this way, the secret keys keep changing dynamically,without knowing the correct historical data, an attacker cannot start a successful conversation with the administration server.

2. Literature Review

here reviewed three categories of work, searchable encryption, secure keyword search in cloud computing, and order preserving encryption.Searchable encryption:The earliest attempt of searchable encryption was made by Song et al. In [3], they propose to encrypt each word in a file independently and allow the server to find whether a single queried keyword is contained in the file without knowing the exact word. This proposal is more of theoretic interests because of high computational costs. Go het al. propose building a keyword index for each file and using Bloom filter to accelerate the search [4]. The searchable encryption cares mostly about single keyword search or Boolean keyword search. Extending these techniques for ranked multi-keyword search will incur heavy computation and storage costs.

2.1 Related work :

Secure keyword search in cloud computing :The privacy concerns in cloud computing motivate the study on secure keyword search. Wang et al.first defined and solved the secure ranked keyword search over encrypted cloud data. they proposed a scheme that returns the top-k relevant files upon a single keyword search. further proposed privacy-assured similarity search mechanisms over outsourced cloud data. In [20], we proposed a secure, efficient, and distributed keyword search protocol in the geodistributed cloud environment.The system model of these previous works only consider one data owner, which implies that in their solutions, the data owner and data users can easily communicate and exchange secret information. When numerous data owners are involved in the system, secret information exchanging will cause considerable communication This paper seeks a solution scheme to maximally relax the requirements for data owners and users, so that the scheme could be suitable for a large number of cloud computing users.

Order preserving encryption :The order preserving encryption is used to prevent the cloud server from knowing the exact relevance scores of keywords to a data file. The early work of Agrawal et al. proposed an Order Preserving symmetric Encryption (OPE) scheme where the numerical order of plain texts is preserved. Boldyreva et al. further introduced a modular order preserving encryption in . Yi et al proposed an order p- reserving function to encode data in sensor networks. Popa et al. [36recently proposed an ideal-secure order-preserving encryption scheme. Kerschbaum etal. Further proposed a scheme which is not only idea-secure but is also an efficient order-preserving encryption scheme. However, these schemes are not additive order preserving. As a complementary work to the previous order preserving work, we propose a new additive order and privacy preserving functions (AOPPF). Data owners can freely choose any function from an AOPPF family to encode their relevance scores. The cloud server computes the sum of encoded relevance scores and ranks them based on the sum.

A view of cloud computing: M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. Privacy preserving public auditing for secure cloud storage. this usually implies that one has to sacrifice functionality for security. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions.Secure conjunctive keyword search over encrypted data. P. Golle, J. Staddon, and B. Waters study the setting in which a user stores encrypted documents (e.g. e-mails) on an untrusted server. In order to retrieve documents satisfying a certain search criterion, the user gives the server a capability that allows the server to identify exactly those documents. Work in this area has largely focused on search criteria consisting of a single keyword. If the user is actually interested in documents

containing each of several keywords (conjunctive keyword search) the user must either give the server capabilities for each of the keywords individually and rely on an intersection calculation. TITLE: Achieving efficient conjunctive keyword searches over encrypted data. L. Ballard, S. Kamara, and F. Monrose. presents two provably secure and efficient schemes for performing conjunctive keyword searches over symmetrically encrypted data. Our first scheme is based on Shamir Secret Sharing and provides the most efficient search technique in this context to date. Although the size of its trapdoors is linear in the number of documents being searched, we empirically show that this overhead remains reasonable in practice. Nonetheless, to address this limitation we provide an alternative based on bilinear pairings that yields constant size trapdoors. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication.

2.2 Summery of related review:

In reviewed literature observed, Companies with large batch-oriented tasks can get results as quickly as their programs. Support hidden queries, the algorithms present are simple, fast for a document of length, the encryption and search. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.The gap identified is investigating privacy, low efficiency, the setting where only the owner of the data is capable of submitting search queries. Approach is computationally low efficient, even when dealing with large datasets and keyword sets. Unsafe fuzzy keyword search within a multi-owner framework as one of the study's topics. On the other hand, it plans to use this technique on private clouds too. To fill this gap in research, need to work with advanced model for keyword search of cloud computing with data security.

3 Proposed system

Proposed PRMSM, a privacy preserving ranked multi-keyword search protocol in a multi-owner cloud model . To enable cloud servers to perform secure search without knowing the actual value of both keywords and trapdoors, we systematically construct a novel secure search protocol. As a result, different data owners use different keys to encrypt their files and keywords. Authenticated data users can issue a query without knowing secret keys of these

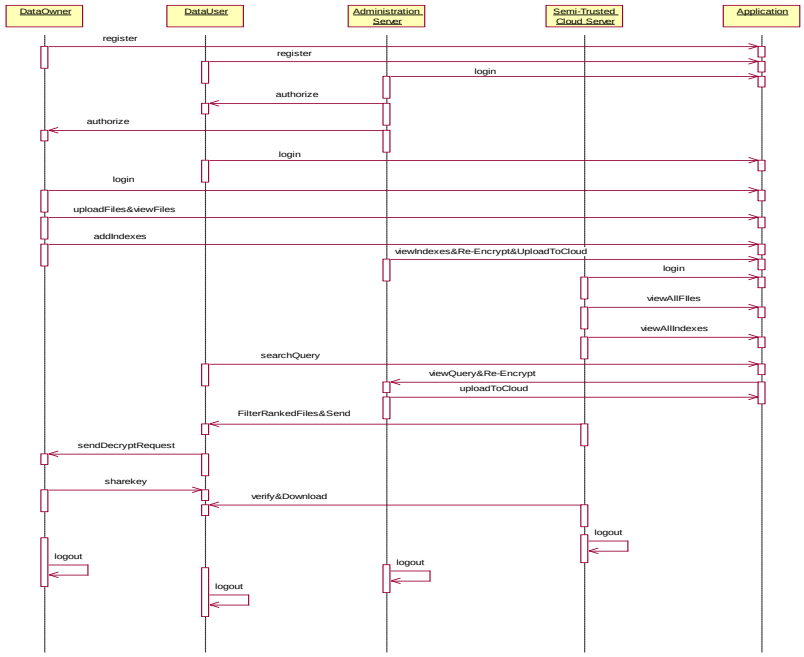

Fig 2: Sequence diagram

different data owners. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a new additive order and privacy preserving function family, which helps the cloud server return the most relevant search results to data users without revealing any sensitive information.UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. the goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UMLThe UML uses mostly graphical notations to express the design of software projects. It will use ,use case diagram, class diagram Sequence diagram and about A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order shown in fig 2. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

4. Comparative of results

Algorithms like: RSA, DES, AES, Blowfish have been used and comparative find out about amongst them have additionally been introduced to make sure the safety of records on cloud ,AES is used broadly now-a-days for safety of cloud. Implementation idea states that First, User decides to use cloud offerings and will migrate his facts on cloud. Then User submits his offerings necessities with Cloud Service Provider (CSP) and chooses first-class particular offerings provided by means of provider.AES regarded as excellent in phrases of safety and execution time and reminiscence utilization is much less in contrast to different algorithms.The Data Encryption Standard (DES) is a block cipher. it encrypts statistics in blocks of dimension sixty four bits each. That is sixty four bits of undeniable textual content goes as enter to DES, which produces sixty four bits of cipher text.The use of 56-bit keys: 56-bit key is used in encryption, there are 256 viable keys. A brute pressure assault on such range of keys is impractical.Blowfish is recognized to be inclined to assaults on reflectively vulnerable keys. This potential Blowfish customers have to cautiously pick out keys as there is a type of keys recognized to be weak, or swap to extra present day picks like the Advanced Encryption Standard. Blowfish fits purposes the place the key stays regular for a lengthy time .AES regarded as satisfactory in phrases of protection and execution time and reminiscence utilization is much less in contrast to different algorithms.comparison of various methods for keyword search shown below in table 1.

Table 1: Comparison of Various methods for keyword search of cloud computing

S. No	Algorithm	Based on keyword searching	clustering	Remarks
1	AES	yes	yes	User outsourced the index and the encrypted File on the cloud server
2	ECC	yes	yes	User can upload the file with index after encryption process
3	OPSE	No	yes	User can upload the index and the encrypted Files on the cloud server
4	IBE	yes	yes	User upload the index and the encrypted File on the cloud server
5	Symmetric key Encryption	yes	yes	User upload cluster index, document index & encrypted document
6	Proposed	yes	yes	Use van upload index, encrypted with security .

5. Conclusion

When looks into the problem of secure multi-keyword search for multiple users and data owners in cloud computing environments, In contrast to earlier research, this system enables legitimate users to conduct quick, safe, secure, and easy searches over the data of multiple data owners. In order to successfully authenticate data users and identify attackers who steal the secret key and conduct unauthorized searches, it present a novel data user authentication protocol and a special dynamic secret key generation mechanism. This carefully developed a novel safe search protocol that allows the cloud server to safely search through data encrypted with different secret keys that are owned by multiple parties. it offers a cutting-edge method for sorting search results while safeguarding the confidentiality of relevance ratings between files and keywords.proposes a novel family of Privacy Preserving and Additive Order Functions. and also show that this approach is computationally efficient, even when dealing with large datasets and keyword sets. Planed to investigate safe fuzzy keyword search within a multi-owner framework as one of the study's topics. On the other hand, it plans to use this technique on private clouds too.

6. References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communication of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[3] D.Song, D.Wagner, and A.Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE International Symposium on Security and Privacy (S&P'00), Nagoya, Japan, Jan. 2000, pp. 44–55.

[4] E. Goh. (2003) secure indexes. [Online]. Available: http://eprint.iacr.org/

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. ACM CCS'06, VA, USA, Oct. 2006, pp. 79–88.

[6] D. B. et al., "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," EUROCRYPT, vol. 43, pp. 506–522, 2004.

[7] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Applied Cryptography and Network Security (ACNS'04), Yellow Mountain, China, Jun. 2004, pp. 31–45.

[8]L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. Information and Communications Security (ICICS'05), Beijing, China, Dec. 2005, pp. 414–426.

[9]C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, Jun. 2010, pp. 253–262.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy preserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM'11, Shanghai, China, Apr. 2011, pp. 829–837.

[11] https://www.researchgate.net/publication/326077495

[12] https://www.researchgate.net/publication/333609774_A2190058119_K_Ramesh_Babu#fullTextFileContent.