iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4533

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Fulfilling Secure, General, and Fine-Grained Question happen Affirmation for Secure Interest Plot over Mixed Cloud Data

S. Anitha[1], Mrs. R. Uma Mageshwari[2], Dr. K. Ravikumar[3]
[1, 2, 3]*Rrase college of engineering, vanchuvancherry*

Abstract: ***Secure search techniques over encrypted cloud data allow an authorized user to query data files of interest by submitting encrypted query keywords to the cloud server in a privacy-preserving manner. However, in practice, the returned query results may be incorrect or incomplete in the dishonest cloud environment. For example, the cloud server may intentionally omit some qualified results to save computational resources and communication overhead.***
Thus, a well-functioning secure query system should provide a query results verification mechanism that allows the data user to verify results.
In this paper, we design a secure, easily integrated, and fine-grained query results verification mechanism, by which, given an encrypted query results set, the query user not only can verify the correctness of each data file in the set but also can further check how many or which qualified data files are not returned if the set is incomplete before decryption. The verification scheme is loose-coupling to concrete secure search techniques and can be very easily integrated into any secure query scheme. We achieve the goal by constructing secure verification object for encrypted cloud data.
Furthermore, a short signature technique with extremely small storage cost is proposed to guarantee the authenticity of verification object and a verification object request technique is presented to allow the query user to securely obtain the desired verification object. Performance evaluation shows that the proposed schemes are practical and efficient.
Keywords: Cloud computing, Query results verification, secure query, Verification object.

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Driven by the abundant benefits brought by the cloud computing such as cost saving, quick deployment, flexible resource configuration, etc., more and more enterprises and individual users are taking into account migrating their private data and native applications to the cloud server.

A matter of public concern is how to guarantee the security of data that is outsourced to a remote cloud server and breaks away from the direct control of data owners. Encryption on private data before outsourcing is an effective measure to protect data confidentiality.

However, encrypted data make effective data retrieval a very challenging task. To address the challenge (i.e., search on encrypted data), Song et al. first introduced the concept of searchable encryption and proposed a practical technique that allows users to search over encrypted data through encrypted query keywords in. Later, many searchable encryption schemes were proposed based on symmetric key and public-key setting to strengthen security and improve query efficiency.

Recently, with the growing popularity of cloud computing, how to securely and efficiently search over encrypted cloud data becomes a research focus.

Some approaches have been proposed based on traditional searchable encryption schemes. In which aim to protect data security and query privacies with better query efficient for cloud computing. However all of these schemes are based on an ideal assumption that the cloud server is an ”honest-but-curious” entity and keeps robust and secure software and hardware environments .As a result, correct and complete query results always be unexceptionally returned from the cloud server when a query ends every time. However, in practical applications, the cloud server may return erroneous or incomplete query results once he behaves dishonestly for illegal profits such as saving computation and communication cost or due to possible software/hardware failure of the server.

II. CONTRIBUTIONS

In this paper extend and reinforce our work in to make it more applicable in the cloud environment and more secure to against dishonest cloud server. The main contributions of this paper are summarized as follows:

A. In this project formally propose the verifiable secure search system model and threat model and design fine grained query results verification scheme for secure keyword search over encrypted cloud data.
B. The propose a short signature technique based on certificate less public-key cryptography to guarantee the authenticity of the verification objects themselves
C. In this project design a novel verification object request technique based on Paillier Encryption, where the cloud server knows nothing about what the data user is requesting for and which verification objects are returned to the user.
D. In this project provide the formal security definition and proof and conduct extensive performance experiments to evaluate the accuracy and efficiency of our proposed scheme.

III. RELATED WORK

A. Secure Search in Cloud Computing

Essentially, the secure search is thus a technique that allows an authorized data user to search over the data owner's encrypted data by submitting encrypted query keywords in a privacy-preserving manner and is an effective extension of traditional searchable encryption to adapt for the cloud computing environment. Motivated by the effective information retrieve on encrypted outsourced cloud data, Wang et al. first proposed a keyword-based secure search scheme and later the secure keyword search issues in cloud computing have been adequately researched which aim to continually improve search efficiency, reduce communication and computation cost, and enrich the category of search function with better security and privacy protection. A common basic assumption of all these schemes is that the cloud is considered to be an "honest-but-curious" entity as well as always keeps robust and secure software/hardware environments. As a result, under the ideal assumption, the correct and complete query results always be unexceptionally returned from the cloud server when a query ends every time.

B. Verifiable Secure Search in Cloud Computing

In practical applications, the cloud server may return erroneous or false search results once he behaves dishonestly for illegal profits or due to possible software/ hardware failure of the cloud server. because of the possible data corruption under a dishonest setting, serval research works have been proposed to allow the data user to enforce query results verification in the secure search fields for cloud computing. In wang et al. applied hash chain technique to implement the completeness verification of query results by embedding the encrypted verification information into their proposed secure searchable index. In sun et al. used encrypted index tree structure to implement secure query results verification functionality. in this scheme, when the query ends, the cloud server returns query results along with a minimum encrypted index tree, then the data user searches this minimum index tree using the same search algorithm as the cloud server did to finish result verification zheng .constructed a verifiable secure query scheme over encrypted cloud data based on attribute-based encryption technique (abe) in the public-key setting .referred to the merkle hash tree and applied pairing operations to implement the correctness and completeness verification of query results for keyword search over large dynamic encrypted cloud data.

IV. BACKGROUND

To clarify our proposed problems, in this section, we present our system model, threat model, used to implement our scheme.

A. System Model

The system model of the secure search over encrypted cloud data usually includes three entities: data owners, data users, and the cloud server, which describes the following scenario: data owners encrypt their private data and upload them to cloud server for enjoying the abundant benefits brought by the cloud computing as well as guaranteeing data security. Meanwhile, the secure searchable indexes are also constructed to support effective keyword search over encrypted outsourced data. An authorized data user obtains interested data files from the cloud server by submitting query trapdoors (encrypted query keywords) to the cloud server, trapdoors and sends the query results to the data user. The above application scenario is based on an ideal assumption that the cloud server is considered as an honest entity and always honestly returns all qualified query results. In this paper, we consider a more challenging model, where the query results would be maliciously deleted or tampered by the dishonest cloud server. When the query

results face the risks that are deleted or tampered, a well-functioning secure query system should provide a mechanism that allows the data user to verify the correctness and completeness of query results. To achieve the results verification goal, we propose to construct secure verification objects for data files that are outsourced to the cloud with encrypted data and secure indexes together. The query results along with corresponding data verification object are returned to the data user when a query ends. The improved system model of verifiable secure search over encrypted cloud data is illustrated in Fig. 1.

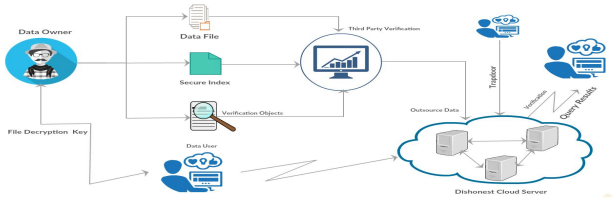


Fig.1.A system model of verifiable secure search and find duplicate file over encrypted cloud.

B. Threat Model

In this paper, compared with the previous works, an important distinction about the threat model is that the cloud is considered to be an un trusted entity. More specifically, first of all, the cloud server tries to gain some valuable information from encrypted data files, secure indexes, and verification objects (e.g., a misbehaving cloud administrator aims at obtaining these information for possible monetary profits). Then, the cloud server would intentionally return false search results for saving computation resource or communication cost. Further, if the cloud server knows a query results verification mechanism is embedded, he may tamper or forge verification objects to escape responsibilities of misbehavior. Similar to the previous works, both data owners and authorized data users are considered to be trusted in our threat model.

V. PROPOSED METHOD

A. Advanced Encryption Standard Algorithm

AES is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits

AES algorithm has 3 steps to implement

1) Constructing Verification Objects
2) Correctness Verification
3) Completeness Verification

VI. QUERY RESULTS VERIFICATION SCHEME

A. Scheme Overview and Problem Definition

When a query ends, both query results and corresponding verification objects are returned to the data user by the cloud server. Upon receiving these data, the data user first checks the authenticity of verification objects and then continued to verify query results according to the verification objects if verification objects pass the test otherwise, the data user rejects this query.

B. The Verification Object Construction

To maximize reduce storage and communication cost and achieve privacy guarantee of the verification objects, in this paper, we will utilize Counting Bloom Filters and the pseudo-random function prfk to construct our verification objects, on which the authorized data user can efficiently perform query results verification.

VII.SECURITY ANALYSIS

A. Security of Verification Object

Similar to the secure index semantic security the security of the verification object aims to capture the notion that the verification object reveals nothing about contents of data files. A more formal and rigorous security definition is the verification object in distinguish ability, which is synoptically described as that, given two verification objects V Ow V Ow0 of set Cw, Cw0 for two different keywords w w0, no polynomial-time adversary A can determine which verification object is for which data file set with probability that is non-negligible greater than 1/2. We use formulation of verification object in distinguish ability to prove the semantic security of our scheme and formally use the following game to define the formulation.

B. Unforgeability of Verification Object Signature

To guarantee the authenticity of the verification objects themselves, a short signature scheme is proposed based on [34] and [36]. We follow the threat model and security definition of certificateless signature scheme by [36] and omit the unforgeability proof of our scheme due to space limitations. Please refer to [36] for detail security proofs calculated using the following equation.

$$W[j] = W_p[j] + W_b[j] + W_c[j] + W_f[j]$$

C. Security of Verification Object Request

We design a secure verification object requesting technique by adopting Paillier encryption. During the whole verification object request process, the cloud server knows nothing about which verification object is requested and which verification object is actually returned since the Paillier encryption is a probabilistic public-key encryption scheme.

VIII. EXPERIMENTAL EVALUATION

We conduct experiments to evaluate the performance of our scheme from four aspects: verification object construction and query results verification, verification object signature and authentication, verification information request generation, and verification accuracy.

A. Performance of Verification Object Construction and Query Results Verification

The time cost of verification object generation for different data files set with different number of data files, we can observe that the size of different data files set has little influence on the time cost of verification object generation. For example, the time cost of generating V O hardware (94ms) and the time cost of generating V O network (99ms) is almost equal, though the size of C network is five times as large as that of C hardware. The reason is that, in our scheme, generating a verification object is mainly determined by HMACMD5 operations, which are involved in both data file insertions and pads. For each data files set, the less the number of data files in the set is, the more random elements is needed to pad for constructing its verification object. Thus the total number of HAMC-MD5 operations will keep the same for each set of data files containing a certain keyword. In addition, the execution time is almost zero of 7 hash functions in H when hashing a small string of length 128 bits. In experiments, the random pad elements are also picked up from RFC randomly for each verification object.

B. Performance of Verification Object Request

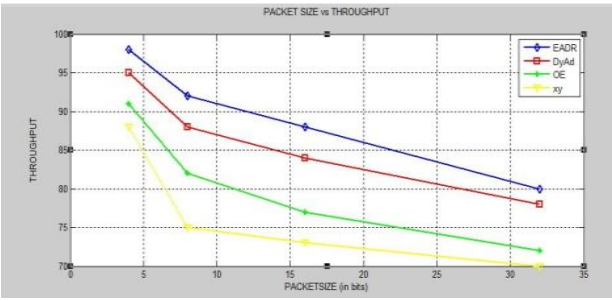
Recall that a data user securely obtains the desired
verification object by three steps, during the whole process, the Paillier encryption is used. First, the data user encrypts request information according to the requested keyword and keywords dictionary W. Second, the cloud server generates encrypted desired verification object according to submitted request information and the outsourced
verification objects set f (_jjV O) wgw2W. Third,
the data user decrypts the encrypted desired verification object returned by the cloud server.

C. Verification Accuracy

Essentially, the constructed verification object is the Bloom Filter, which can incur the false positive. This means that our scheme may cause incorrect query results to pass the correctness verifications. To numerically evaluate the verification accuracy, we first define several verification events. Given a returned query results set Rw of the query keyword w and corresponding
verification object V Ow, for each result c 2 Rw, if a verification Event occurs, then the Event is set as 1, obviously,

Number of kerword in W

(a)



Number of data file in C

(b)

Fig. (a) The time cost of generating encrypted desired verification object for cloud server: (a) for different number of keywords in the keyword dictionary W, and (b) for different number of data files in Cw with the fixed dictionary,(W) = 70.

Fig (b) The evaluation of verification accuracy: (a) for different number of hash functions in Bloom Filter, R network contains 300 correct query results and 500 incorrect query results, and (b) for different number of incorrect query results. in Rnetwork with the fixed hash functions (l=7),Rnetwork contains 300 correct query reuslts.

IX. CONCLUSION

In this paper, these propose a secure, easily integrated, and fine-grained query results verification scheme for secure search over encrypted cloud data. Different from previous works, our scheme can verify the correctness of each encrypted query result or further accurately find out how many or which qualified data files are returned by the dishonest cloud server. A short signature technique is designed to guarantee the authenticity of verification object itself. Moreover, we design a secure verification object request technique, by which the cloud server knows nothing about which verification object is requested by the data user and actually returned by the cloud server. Performance and accuracy experiments demonstrate the validity and efficiency of our proposed

REFERENCES

[1] M. Ahluwalia, A.Gangopadhyay, and Z. Chen, "Preserving Privacy in Mining Quantitative Association Rules," International Journal of Information Security and Privacy, 2010.

[2] M.Ahluwalia,R.Gupta,A.Gangopadhyay, Y. Yesha, and M. McAllister,"Target-Based Database Synchronization," presented at the 25th ACM Symposium on Applied Computing, Sierre, Switzerland, 2010

[3] W. K. Wong, D. W. Cheung, E. Hung, and H. Liu, "Protecting privacy in incremental maintenance for distributed association rule mining," PAKDD'08: Proceedings of the 12th Pacific-Asia conference on Advances in knowledge discovery and data mining, 2008.

[4] J.-L. Lin and J.Y.-C. Liu, "Privacy preserving item set mining through fake transactions," in Proceedings of the 2007 ACM symposium on applied computing. Seoul, Korea: ACM Press, 2007, pp. 375-379.

[5] Z.-Y. Chen and G.-H.Liu, "Quantitative Association Rules Mining Methods with Privacy-preserving," Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005.PDCAT 2005, pp. 910-912, 2005.

[6] A. Evfimevski, R. Srikant, R. Agrawal, and J. Gehrke, "Privacy preserving mining of association rules," 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'02), pp. 217 -228, 2002.

[7] S. Rizvi and J. R. Haritsa, "Maintaining Data Privacy in Association Rule Mining," VLDB, pp. 682-693, 2002.

[8] D. W. Cheung, S. D. Lee, and B. Kao, "A general incremental technique for maintaining discovered association rules," Proc. 5th Int. Conf. Database Systems Advanced Applications, pp. 1-4, 1997.

[9] J. S. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," 8th ACM SIGKDD Inter-national Conference on Knowledge Discovery and Data Mining, pp. 639 -644, 2002.

[10] M. Naveed, M. Prabhakaran, and C. A. Gunter, "Dynamic searchable encryption via blind storage," in IEEE S&P, May 2014, pp. 639–654.

[11] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in IEEE ICDCS, 2010, pp. 253–262.

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

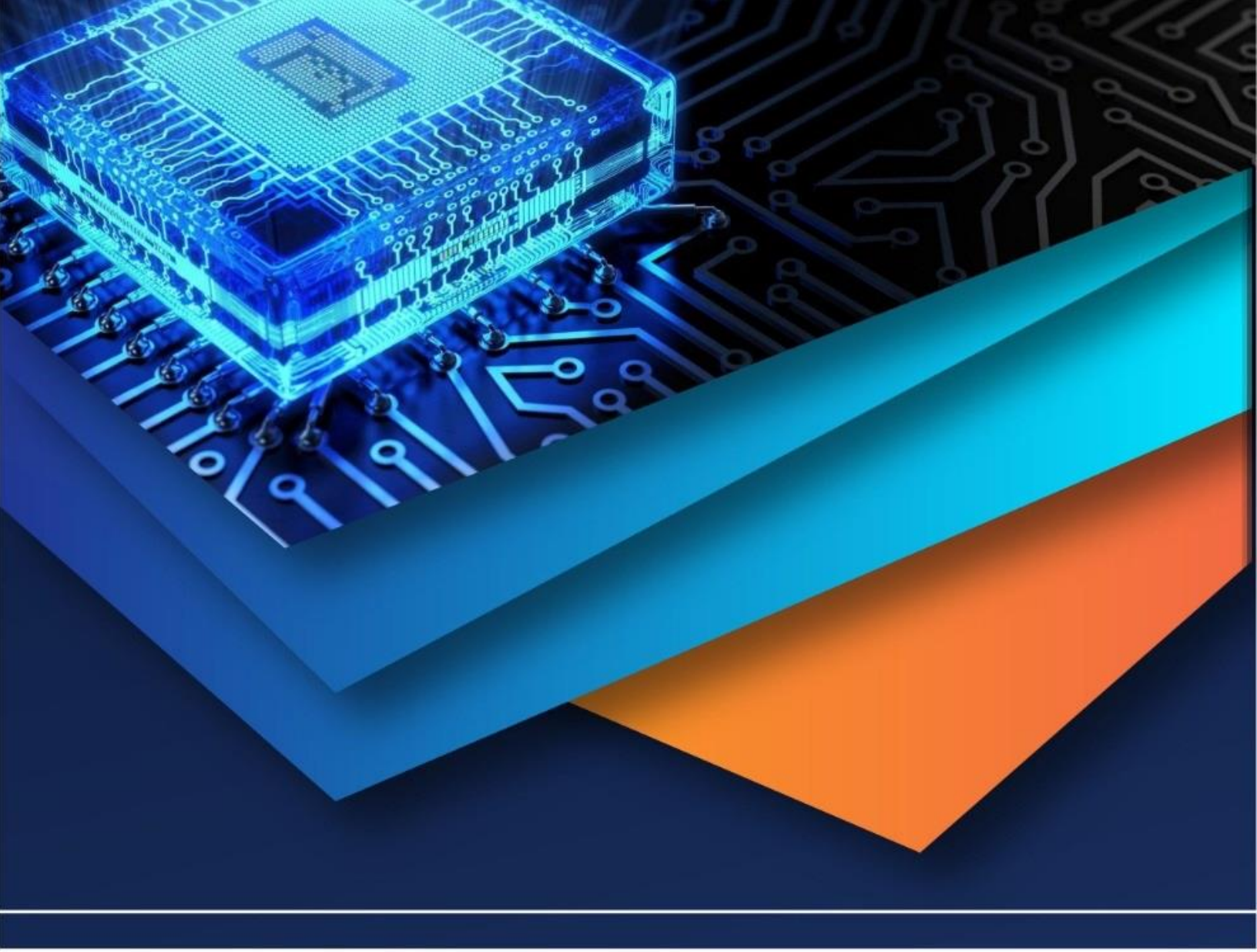
[13] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in ACM ASIACCS, 2013.

[14] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi keyword fuzzy search over encrypted data in the cloud," in IEEE INFOCOM, 2014, pp. 2112–2120.

[15] W. Zhang, S.Xiao, Y. Lin, J. Wu, and S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing," IEEE Transactions on Computers, vol. 65, no. 5, pp. 1566–1577, May 2016.

[16] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Transactions on Parallel and Distributed System, vol. 27, no. 2, pp. 340–352, 2015.

[17] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Transactions on Communications, vol. E98-B, no. 1, pp. 190–200, 2015.
[18] H. Yin, Z. Qin, L. Ou, and K. Li, "A query privacy enhanced and secure search scheme over encrypted data in cloud computing," Journal of Computer and System Sciences, http://dx.doi.org/10.1016/j.jcss.2016.12.003.
[19] B. Wang, B. Li, and H. Li, "Oruta" Privacy-preserving public auditing for shared data in the cloud," IEEE Transactions on Cloud Computing, vol. 2, no. 1, pp. 43–56, 2014.
[20] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467–1479, 2012.
[21] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, and Y. T. Hou, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, pp. 3025–3035, 2014.
[22] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: Verifiable attribute based keyword search over outsourced encrypted data," in IEEE INFOCOM, May 2014, pp. 522–530.
[23] W. Sun, X. Liu, W. Lou, Y. T. Hou, and H. Li, "Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data," in IEEE INFOCOM, April 2015, pp. 2110–2118.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY