International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

Efficient and Verifiable Queries over Encrypted Data in Cloud

Sudha L[1], Manoj R[2], Prasanth B[4], Praveen A[4]

[1] *Assistant Professor, Dept. of Computer Science Engineering, S.A.Enginnering college, TN, India*
[2] *Student, Dept. of Computer Science Engineering, S.A.Enginnering college, TN, India*
[3] *Student, Dept. of Computer Science Engineering, S.A.Enginnering college, TN, India*
[4] *Student, Dept. of Computer Science Engineering, S.A.Enginnering college, TN, India*

Abstract - *In pursuit of secure strategies over encoded cloud data enable an approved client to inquiry information documents of enthusiasm by submitting scrambled question catchphrases to the cloud server in a protection safeguarding way. Practically, the returned question results might be deficient in the exploitative cloud condition. The cloud server may prevent some qualified outcomes to spare computational assets and correspondence overhead. In this manner, a well-functioning Safe Inquiry framework ought to give a question comes about check system that enables the information client to confirm comes about. we outline a protected, effectively incorporated, and fine-grained question comes about confirmation instrument, by which, given an encoded inquiry comes about set, the question client not exclusively can check the rightness of every information record in the set yet in addition can additionally check what number of or which qualified information documents are not returned if the set is inadequate before unscrambling. We accomplish the objective by building secure check question for scrambled cloud information.*

***Key Words*: searchable symmetric encryption, encrypted cloud data, verification, data dynamic, symmetric-key cryptography.**

1.INTRODUCTION

Cloud computing provides a way to access applications on the Internet as applications. It allows you to create, configure and customize applications online. Public cloud systems and services allow for easy access to the public. Public cloud may be less secure due to its openness, e.g., email. Private Cloud allows you to access systems and services within an organization. It offers increased security due to its unique nature. Community cloud allows organizations and services to access systems and services. Hybrid Cloud is a combination of public and private cloud. However, critical operations are performed using private cloud, while non-critical operations are performed using public cloud. Risks Although Cloud Computing is a great innovation in the world of computing, there are downsides to cloud computing. Some of them are discussed below: SECURITY & PRIVACY: It is the biggest problem in cloud computing. As data and infrastructure management in cloud is provided by third-party, it is always a risk to handover sensitive information to such providers. Although cloud computing vendors ensure more secure protected accounts, any sign of security breach would result in loss of clients and businesses. LOCK-IN: It is very difficult for the customers to switch from one Cloud Service Provider (CSP) to another. It results in dependency on a particular CSP. ISOLATION FAILURE: This involves the failure of isolation mechanism that isolates storage, memory, routing between the different end users. In a search process, for returned query results that contain multiple encrypted data files, a data user may want to check the correctness of each encrypted data file (thus, he wants to check how many) or any valid data files on the earth have not been returned if the cloud server deliberately omits some query results, removing the wrong results and retaining the correct ones. This information can be viewed as a hard evidence to punish the cloud server. Because querying and verification are implemented in an encrypted environment, achieving elegant verification is challenging. We proposed a secure and elegant query result verification scheme by creating a validation object for encrypted outsourced data files.

2. RELATED WORKS

In this paper [8], the authors investigate the searchable encryption problem in the presence of a malicious server, which requires verifiable search to provide users with the ability to detect potential malpractices. Verifiable and dynamically fuzzy keyword search (VDFS) Secure Fuzzy Keyword Search, Program to Provide Update the outsource document collection and authenticity of search results. In this paper [9], a new scheme a novel verifiable fuzzy keyword search scheme over encrypted cloud data is proposed. The Authors construct a linked list for each keyword and generate a fuzzy keyword set. To decrease the computation cost and the storage space, they generate one index vector for each fuzzy keyword set, instead of each fuzzy keyword. Security analysis and experiment evaluation are made to show that the proposed schemes are secure and efficient. In this paper [10], the authors devised a basic cryptographic primitive called as attribute-based keyword search over hierarchical data (ABKS-HD) scheme by using the ciphertext-policy attribute-based encryption (CP-ABE) technique, they also proposed two improved schemes (ABKS-HD-I,ABKS-HD-II) for supporting multi-keyword search and user revocation. General security analysis confirms that these schemes are more secure against both chosen-plaintext attack (CPA) and chosen-keyword attack (CKA). In this paper [11], the authors focus on the aspect of

cloud storage auditing. They investigate how to decrease the damage of the client's key exposure in cloud storage auditing They redefine the security model of auditing protocol with key-exposure resilience. They developed the binary tree structure and the pre-order traversal technique to update the secret keys for the client. They also develop a novel authenticator construction to support the security. The security and performance results show that the proposed protocol is more secure and efficient. In this paper [12], the authors aim to verify the correctness of the retrieved data in case of fault in cloud server that leads to computational error. This is achieved by designing a new scheme Verifiable Privacy-preserving keyword Search scheme, by integrating homomorphic MAC technique with a privacy-preserving multi-keyword search scheme. This enables the end user to verify the correctness of search result efficiently. In this paper [13], attribute-based encryption is a technique for fine-grained access control of encrypted data in a cloud storage. However, decryption is usually too expensive for end users. So as to reduce overhead involved in decrytion, Green et al. provided a suggestion to outsource the major part of the decryption work without revealing the data or private keys. They proposed a key blinding technique to outsource the decryption without leaking data or secret keys. This paper proposes a method to overcome the above issue by reducing the computational cost and bandwidth to nearly half. In this paper [14], the authors propose publicly auditable cloud data storage can help with this new cloud the economy is fully established. A trusted company with public auditing skills the expertise and skills that data owners lack are a external audit party to assess the risk of outsourced data when needed. We describe the approaches and system requirements that must be brought consider, and outline such publicly addressed challenges an auditable secure cloud storage service is a reality. In this paper [15], the authors propose a Verifiable Ranked Searchable Symmetric Encryption (VRSSE) scheme that allows a user to perform best-K searches on a dynamic file collection while verifying the correctness of the results. VRSSE is constructed based on the ranked inverted index, which has multiple inverted lists that connect sets of file nodes relating the exact keyword. More experiments on real data sets show the efficiency and effectiveness of this proposed scheme. In this paper [6], the author addresses the challenging problem of privacy-protecting multi-core data search on cloud computing (MRSE) encrypted data. We choose the effective harmonic level of "cohesiveness" in a number of different key terms. They first propose a basic idea for MRSE based on secure internal product computation, and then offer two MRSE programs that are significantly improved to meet different stringent privacy requirements in two different threat models. To further enhance the search experience of the data search service, these two programs are further expanded to support the search engine. In this paper [7], the author propose a multi-phrase search on encrypted cloud data, which also supports dynamic update functions such as adding or deleting files. The relevant score evaluation model is used in the search process on the client side to sort the results and protect the privacy of the appropriate data. In this paper [5], the author proposes a seamless, integrated, machine-readable, semantic representation of cloud services, forms, equipment, and their combinations. Portability and portability issues often arise, and this can only worsen if customers choose to use services from different providers. In this study, we propose a seamless, integrated, machine-readable, semantic representation of cloud services, forms, equipment and their combinations. In this paper [4], it is very difficult for Cloud Service Providers (CSPs) to detect and remove such excesses without affecting the quality of service (QoS) because they do not know the actual performance of the business service, but only on IT services. therefore have advanced analytics to solve problems and accelerate real-time cloud adoption for large corporations in the context of meeting (or exceeding) business service level objectives (SLOs) and reducing cloud subscription cost (OPEX) for businesses. In this paper [3], the author offers a verifiable privacy-protecting multi-key text search (MTS) program with similarity-based data to solve this problem. To support multiple keyword searches and search result ranking, we propose to build a time frequency and vector space model based on the cosine similarity measure to achieve higher search result accuracy. In this paper [2], the author proposes a global transformation that will transform any anonymous identity-based encryption (IBE) program into a secure PEFKS program. Following the general construction, if the main space space is a polynomial scale, we instantiate the first PEFKS program that is proven safe under the KGA. In this Paper [1], the author first identify the difficulties and security problems of live extensions with fully updated data updates from previous works, and then show how to create an elegant verification scheme for seamless integration of these two key features in our protocol design.

3. PROPOSED SYSTEM

Secure and elegant query results verification scheme by creating a validation object for encrypted outsourced data files. When the query ends, the query results set together with the corresponding validation object are returned together, by which the query user can accurately verify:

1. The correctness of each encrypted data file in the results set,
2. How many eligible data files were not returned and
3. Which eligible data files were not retrieved.

Furthermore, our proposed verification scheme is Concrete Safe Query Plans are lightweight and loose-fitting and can be easily fitted into any secure query program for cloud computing.

ADVANTAGE

- We propose a verifiable secure search system model and threat model and design a simple query results verification scheme for secure keyword search in encrypted cloud data.

- We propose a short signature technique based on certified low-key cryptography to ensure the validity of verification objects.
- We provide a systematic safety definition and proof and conduct comprehensive performance tests to evaluate the accuracy and effectiveness of our proposed project.

4. CONCLUSIONS

We propose a secure, easily integrated, and elegant query results verification scheme for secure search in encrypted cloud data. Different from previous works, our program can verify the correctness of each encrypted query result, or more accurately determine how or what credible data files are returned by a trusted cloud server. A short signature technique is designed to ensure the validity of the verification object. Furthermore, We are designing a secure verification object request mechanism so that the cloud server knows what verification object data is requested by the user and is actually being returned by the user and is actually being returned by the cloud server. Performance and accuracy tests also prove the validity of our propose scheme.

REFERENCES

[1] Qian Wang, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011.

[2] Peng Xu, Hai Jin, "Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack" in IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 11, NOVEMBER 2013.

[3] Wenhai Sun, "Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking" in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 11, NOVEMBER 2014.

[4] Jyotiska Nath Khasnabish, Mohammad Firoj Mithani, "Tier-Centric Resource Allocation in Multi-Tier Cloud Systems" DOI: 10.1109/TCC.2015.2424888, IEEE Transactions on Cloud Computing 2015.

[5] Beniamino Di Martino, Antonio Esposito and Giuseppina Cretella, "Semantic Representation of Cloud Patterns and Services with Automated Reasoning to support Cloud Application Portability", DOI: 10.1109/TCC.2015.2433259, IEEE Transactions on Cloud Computing 2015.

[6] Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou "Privacy-Preserving Multi Keyword Ranked Search over Encrypted Cloud Data" in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014.

[7] C. Guo, X. Chen, Y. M. Jie, Z. J. Fu, M. C. Li and B. Feng, "Dynamic Multi-phrase Ranked Search over Encrypted Data with Symmetric Searchable Encryption," in IEEE Transations on Services Computing, vol. 99, No. 1939, pp. 1-1, 2017.

[8] X. Y. Zhu, Q. Liu and G. J. Wang, "A Novel Verifiable and Dynamic Fuzzy Keyword Search Scheme over Encrypted Data in Cloud Computing," presented at the IEEE Trustcom/BigDataSE/ISPA, pp. 845-851, 2017.

[9] X. R. Ge, J. Yu, C. Y. Hu, H. L. Zhang and R. Hao, "Enabling Efficient Verifiable Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," in IEEE Access, vol. 6, pp. 45725-45739, 2018.

[10] Y. B. Miao, J. F. Ma, X. M. Liu, X. H. Li, Q. Jiang and J. W. Zhang, "Attribute-based keyword search over hierarchical data in cloud computing," in IEEE Transactions on Services Computing, doi:10.1109/TSC.2017.2757467, 2017..

[11] Jia Yu, Kui Ren and Vijay Varadharajan "Enabling Cloud Storage Auditing with Key-Exposure Resistance," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. , NO. , 2014.

[12] Zhiguo Wan and Robert H. Deng, "VPSearch: Achieving Verifiability for Privacy-Preserving Multi-Keyword Search over Encrypted Cloud Data," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 15, NO. 6, NOVEMBER/DECEMBER 2018

[13] Suqing Lin, Rui Zhang, Hui Ma, and Mingsheng Wang, "Revisiting Attribute-Based Encryption WithVerifiable Outsourced Decryption," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 10, OCTOBER 2015

[14] Cong Wang and Kui Ren, Wenjing Lou,Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services ," IEEE Network , July/August 2010

[15] Qin Liu, Xiaohong Nie, Xuhui Liu, Tao Peng, and Jie Wu, "Verifiable Ranked Search Over Dynamic Encrypted Data in Cloud Computing," 978-1-5386-2704-4/17/$31.00 ©2017 IEEE.