ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Special Issue , August 2019

International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

Achieve a Universal and Detailed Query Results Verification for a Secure Search Scheme

M.USHA RANI, M.TIRUPATHAMMA, J.KEERTHI

Asst Prof, Dept of CSE, Sree Vahini Institute of Science and Technology, Tiruvuru, AP, India.

ABSTRACT: As the number of internet users is increasing, Technologies in this area is also developing day by day. Cloud computing is an important paradigm evolved as a recent Technology in IT environment. It is defined on the basis of cloud networking and cloud service provider. Cloud computing is the process of providing computing services i.e. Software services, Networking, Database services and storage facilities over the internet. Major challenge in cloud network is security of data outsourced to it. Many existing Technique have defined data encryption as a method of securing data. In the proposed system, we propose a method of generating verification object using a pseudo-random function generator for each data file stored in the cloud. For data users to access this, admin should provide verification object to each user. If Data Loss and Data Hacking occurs within the cloud storage, verification object of source file will be changed and corresponding admin will get a notification about the same .Thus it provides a double security to data within the cloud storage

KEYWORDS: Pseudo-random function, Encryption, Cloud storage, Networking, Virtualization**,** Query results verification.

I. INTRODUCTION

A. Motivation: 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 [1]. 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 [2]. Encryption on private data before outsourcing is an effective measure to protect data confidentiality [3]. 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 [4]. Later, many searchable encryption schemes were proposed based on symmetric key and public-key setting to strengthen security and improve query efficiency [5], [6], [7], [8], [9], [10], [11],[12]. 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 [13], [14], [15], [16],[17], [18], [19], [20], [21], 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/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 [22].Therefore, the above fact usually motivates data users to verify the correctness and completeness of query results. Some researchers proposed to integrate the query results verification mechanisms to their secure search schemes [23], [24], [25], [26], (e.g., embedding verification information into the

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Special Issue , August 2019
International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

specified secure indexes or query results). Upon receiving query results, data users use specified verification information to verify their correct ness and completeness. There are two limitations in these schemes:
1) These verification mechanisms provide a coarse-grained verification, i.e., if the query result set contains all qualified and correct data files, then these schemes reply yes, otherwise reply no. Thus, if the verification algorithm outputs no, a data user has to abort the decryption for all query results despite only one query result is incorrect.
2) These verification mechanisms are generally tightly coupled to corresponding secure query constructions and have not universality.

B. Our Contributions: In this paper, we extend and reinforce our work in [27] 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:
1) We formally propose the verifiable secure search system model and threat model and design a fine-grained query results verification scheme for secure keyword search over encrypted cloud data.
2) We propose a short signature technique based on certificate less public-key cryptography to guarantee the authenticity of the verification objects themselves.
3) We 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
4) We provide the formal security definition and proof and conduct extensive performance experiments to evaluate the accuracy and efficiency of our proposed scheme.

II. 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 [13] and later the secure keyword search issues in cloud computing have been adequately researched [14], [15], [16], [17], [18],[19], [20], [21], 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 [23], 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 [24], 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 et al. [25] constructed a verifiable secure query scheme over encrypted cloud data based on attribute-based encryption technique (ABE) [28] in the public-key setting. Sun et al. [26] referred to the Markel 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. However, these secure verification schemes cannot achieve our proposed fine-grained verification goals. Furthermore, these verification mechanisms are generally tightly coupled to corresponding secure query schemes and have not universality.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Special Issue , August 2019
International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

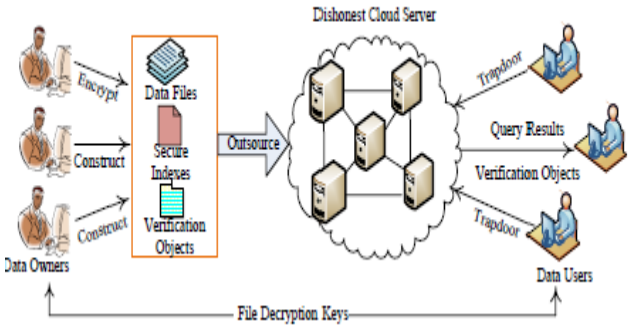

Fig. 1. A system model of verifiable secure search over encrypted cloud data.

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.

III. CONCLUSION

In this paper, we 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 scheme.

REFERENCES

[1] P. Mell and T. Grance, “The nist definition of cloud computing,” http://dx.doi.org/10.602/NIST.SP.800-145.
[2] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.
[3] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Springer RLCPS, January 2010.
[4] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in IEEE Symposiumon Security and Privacy, vol. 8, 2000, pp. 44–55.
[5] E.-J.Goh, “Secure indexes,” IACR ePrint Cryptography Archive, http://eprint.iacr.org/2003/216, Tech. Rep., 2003.
[6] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano,“Public-key encryption with keyword search,” in EUROCRYPR,2004, pp. 506–522.
[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved deinitions and efficient constructions,”in ACM CCS, vol. 19, 2006, pp. 79–88.
[8] M. Bellare, A. Boldyreva, and A. O’Neill, “Deterministic and efficiently searchable encryption,” in Springer CRYPTO, 2007.
[9] K. Kurosawa and Y. Ohtaki, “Uc-secure searchable symmetric encryption,” Lecture Notes in Computer Science, vol. 7397, pp. 258–274, 2012.
[10] P. Xu, H. Jin, Q. Wu, and W. Wang, “Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack,” IEEE Transactions on Computers, vol. 62, no. 11,pp. 2266–2277, 2013.