DESIGN AND IMPLEMENTATION OF QUERY RESULT VERIFICATION MECHANISM WITH FINE-GRAINED ACCESS CONTROL IN CLOUD COMPUTING

K VENKATA RATNAM[1], P.VINAY[2]

[1]Assoc. Professor, Dept. of MCA, Audisankara College of Engineering and Technology, Andhra Pradesh, India.

[2]PG Scholar, Dept. of MCA, Audisankara College of Engineering and Technology, Andhra Pradesh, India.

Abstract – Secure hunt strategies over scrambled cloud information permit an approved client to question information records of interest by submitting encoded question catchphrases to the cloud server in a protection safeguarding way. In any case, by and by, the returned question results perhaps mistaken or fragmented in the untrustworthy cloud climate. In this paper, we plan a solid, effortlessly coordinated, and fine-grained question results confirmation component, by which, given a scrambled inquiry results set, the inquiry client not exclusively can confirm the rightness of every information document in the set yet in addition can additionally check the number of or which qualified information records are not returned in the event that the set is fragmented before decoding. The check conspire is free coupling to concrete secure inquiry procedures and can be handily incorporated into any protected question plot. We accomplish the objective by developing secure confirmation object for encoded cloud information. Moreover, a short signature procedure with minuscule capacity cost is proposed to ensure the legitimacy of confirmation object and a check object demand method is introduced to permit the question client to safely get the ideal check object.

Index terms – Results object verification, Cloud computing, Keyword Searching.

I. INTRODUCTION

Driven by the plentiful advantages brought by the distributed computing like expense saving, speedy organization, adaptable asset arrangement, and so on, an ever increasing number of ventures and individual clients are considering relocating their confidential information and local applications to the cloud

waiter. A question of public concern is the way to ensure the security of information that is moved to are bit cloud server and splits from the immediate control of information proprietors [2]. Encryption on confidential information prior to reevaluating is a powerful measure to safeguard information classification [3]. Nonetheless, scrambled information make compelling information recovery an extremely difficult undertaking. To address the test (i.e., search on encoded information), Song et al. first presented the idea of accessible encryption and proposed a down to earth procedure that permits clients to look through over encoded information through scrambled question catchphrases in [4]. Afterward, numerous accessible encryption plans were proposed in light of symmetric key and public-key setting to fortify security and further develop question productivity. As of late, with the developing prominence of distributed computing, how to safely and proficiently search over encoded cloud information turns into an exploration center. A few methodologies have been proposed in view of customary accessible encryption plans in, which mean to safeguard information security and question protective measures with better question proficient for distributed computing.

Notwithstanding, these plans depend on an ideal presumption that the cloud server is an" fair however inquisitive" element and keeps powerful and secure programming/equipment conditions. Subsequently, right and complete question results forever be unremarkably gotten back from the cloud server when an inquiry closes without fail. In any case, in viable applications, the cloud server might return wrong or deficient question results once he acts unscrupulously for unlawful benefits, for example, saving calculation and correspondence cost or because of conceivable programming/equipment disappointment of the server.

II. BACKGROND WORK

Basically, the protected hunt is hence a procedure that permits an approved information client to look through over the information proprietor's scrambled information by submitting encoded question catchphrases in a security saving way and is a viable expansion of conventional accessible encryption to adjust for the distributed computing climate. Inspired by the successful data recover on encoded rethought cloud information, Wang et al. first proposed a catchphrase based secure pursuit conspire and later the safe watchword search issues in distributed computing have been enough explored which mean to ceaselessly further

develop search effectiveness, lessen correspondence and calculation cost, and enhance the classification of search capability with better security and security. A typical essential presumption of this large number of plans is that the cloud is viewed as an "genuine however inquisitive" substance as well as consistently keeps vigorous and secure programming/equipment.

In commonsense applications, the cloud server might return wrong or misleading query items once he acts untrustworthily for unlawful benefits or because of conceivable programming/equipment disappointment of the cloud server. Due to the potential information debasement under an unscrupulous setting, a few exploration works have been proposed to permit the information client to implement question results check in the solid quest fields for distributed computing. Wang et al. applied hash bind method to execute the fulfillment confirmation of question results by installing the encoded check data into their proposed secure accessible record. Sun et al. utilized encoded record tree construction to execute secure question results check usefulness. In this plan, when the question closes, the cloud server returns inquiry results alongside a base scrambled record tree, then, at that point, the information client look through this base file tree involving a similar hunt calculation as the cloud server did to complete outcome check. Zheng et al. built a certain solid question plot over scrambled cloud information in view of property based encryption procedure (ABE) in the public-key setting. Sun et al. alluded to the Merkle hash tree and applied Pairing tasks to carry out the rightness and culmination confirmation of question results for watchword search over enormous unique encoded cloud information. Notwithstanding, these solid check plans can't accomplish our proposed fine-grained confirmation objectives. Moreover, these confirmation instruments are for the most part firmly coupled to relating secure inquiry conspires and have not comprehensiveness.

III. PROPOSED WORK

The framework model of the solid inquiry over encoded cloud information typically incorporates three elements: information proprietors, information clients, and the cloud server, which depicts the accompanying situation: information proprietors scramble their confidential information and transfer them to cloud server for partaking in the bountiful advantages brought by the distributed computing as well as ensuring information security. In the interim, the protected accessible records are likewise developed to help powerful catchphrase search

over scrambled re-appropriated information. An approved information client gets intrigued information documents from the cloud server by submitting inquiry secret entryways (encoded question catchphrases) to the cloud server, who performs search over secure files as indicated by secret entrances and sends the inquiry results to the information client. In this paper, we think about a seriously difficult model, where the question results would be perniciously erased or altered by the exploitative cloud server. At the point when the question results face the dangers that are erased or altered, a well-working secure inquiry framework ought to give an instrument that permits the information client to confirm the rightness and culmination of inquiry results. To accomplish the outcomes check objective, we propose to build secure confirmation objects for information documents that are moved to the cloud with encoded information and secure records together. The inquiry results alongside relating information check object are gotten back to the information client when a question closes. The better framework model of irrefutable secure hunt over encoded cloud information is represented in Fig. 1.

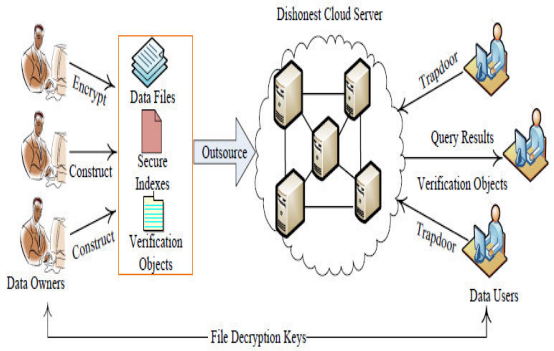

Fig. 1: System Overview

Fig. 2 shows an outline of the inquiry results confirmation process. In short, when a question closes, both inquiry results and relating confirmation objects are gotten back to the information client by the cloud server. After getting these information, the information client first checks the credibility of confirmation items and afterward kept on checking inquiry results as per the confirmation objects in the event that confirmation objects finish the assessment; in any case, the information client dismisses this question.

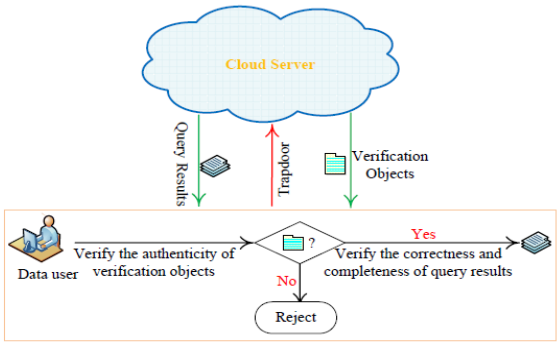

Fig. 2: The process of query results verification

IV. RESULTS

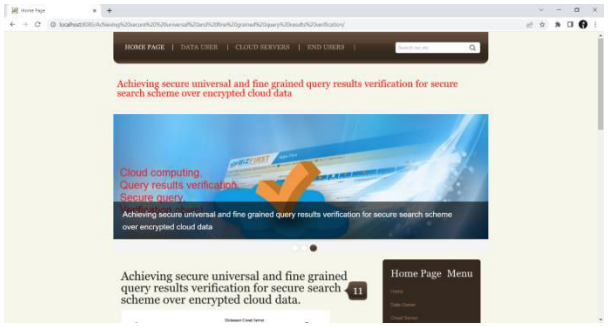

Fig. 3: Home Page

Fig. 4: Data Owner Home

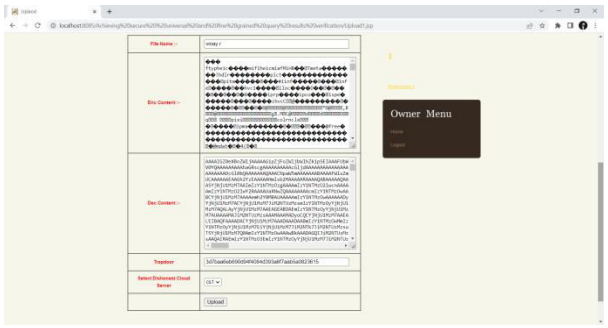

Fig. 5: Upload data into Cloud Server

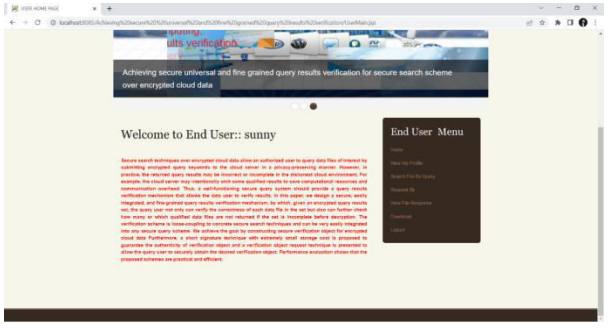

Fig. 6: End User Home

V. CONCLUSION

In this paper, we propose a protected, effectively coordinated, and fine-grained question results confirmation conspire for secure pursuit over encoded cloud information. Not quite the same as past works, our plan can check the rightness of each encoded question result or further precisely figure out the number of or which qualified information records are returned by the untrustworthy cloud server. A short signature strategy is intended to ensure the validness of confirmation object itself. Besides, we plan a solid confirmation object demand strategy, by which the cloud server doesn't know anything about which check object is mentioned by the information client and really returned by the cloud server. Our plans support information elements on condition that the refreshing information don't part or consolidation a non-leaf hub in R-tree. Additionally, the cloud server could gain proficiency with the entrance design during executing range inquiries. We trust these difficulties will be defeated in future work.

REFERNCES

[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 publiccloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[3] S. Kamara and K. Lauter, "Cryptographic cloud storage," inSpringer 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.