Volume 2, Issue 12, December-2015, pp. 919-923 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data

[1]G.Lucy,[2] D.Jaya Narayana Reddy,[3]R.Sandeep Kumar

[1]Pursuing M.Tech, CSE Branch, Dept of CSE

[2]Assistant Professor, Department of Computer Science and Engineering

[3]Assistant Professor, Department of Computer Science and Engineering

G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

Abstract: - Utilizing Cloud Computing, people can store their information on remote servers and permit information access to open clients through the cloud servers. As the outsourced information are liable to contain touchy protection data, they are regularly scrambled before transferred to the cloud. This, on the other hand, altogether restrains the ease of use of outsourced information because of the trouble of seeking over the encoded information. In this paper, we address this issue by building up the fine-grained multi-watchword hunt plans over scrambled cloud information. Our unique commitments are three-fold. To begin with, we present the significance scores and inclination elements upon watchwords which empower the exact catchphrase seek and customized client experience. Second, we build up a handy and exceptionally effective multi-catchphrase inquiry plan. The proposed plan can backing entangled rationale seek the blended "AND", "OR" and "NO" operations of catchphrases. Third, we further utilize the ordered sub-lexicons procedure to accomplish better proficiency on list building, trapdoor producing and question. Finally, we examine the security of the proposed plans as far as secrecy of reports, security assurance of file and trapdoor, and unlinkability of trapdoor. Through broad investigations utilizing this present reality dataset, we approve the execution of the proposed plans. Both the security examination and test results show that the proposed plans can accomplish the same security level contrasting with the current ones and better execution as far as usefulness, question multifaceted nature and effectiveness.

Keywords – Searchable encryption, Multi-keyword, Secure Computation on Encrypted Database, Fine-grained, Cloud computing

1. INTRODUCTION

The Cloud Computing regards processing as a utility and leases out the figuring and stockpiling abilities to general society people [1], [2], [3]. In such a system, the individual can remotely store her information on the cloud server, in particular information outsourcing, and after that make the cloud information open for free through the cloud server. This speaks to a more versatile, ease and stable route for open information access on account of the adaptability and high proficiency of cloud servers, and consequently is positive to little enterprises. Note that the outsourced information may contain touchy protection data. It is regularly important to scramble the private information before transmitting the information to the cloud servers [4], [5]. The information encryption, be that as it may, would essentially bring down the ease of use of information because of the trouble of looking over the scrambled information [6]. Essentially encoding the information may even now bring about other security concerns. Case in point, Google Search utilizes SSL (Secure Sockets Layer) to scramble the association between pursuit client and Google server when private information, for example, reports and messages show up in the indexed lists [7]. In any case, if the inquiry client clicks into another site from the query items page, that site may have the capacity to recognize the hunt terms that the client has utilized. On

tending to above issues, the searchable encryption (e.g., [8], [9], [10]) has been as of late created as an essential way to deal with empower seeking over scrambled cloud information, which continues the accompanying operations. Firstly, the information proprietor needs to create a few watchwords as indicated by the outsourced information. These watchwords are then encoded and put away at the cloud server. At the point when a pursuit client needs to get to the outsourced information, it can choose some significant watchwords and send the ciphertext of the chose catchphrases to the cloud server. The cloud server then uses the ciphertext to coordinate the outsourced scrambled catchphrases, and in conclusion gives back the coordinating results to the inquiry client. To accomplish the comparative hunt effectiveness and accuracy over scrambled information as that of plaintext catchphrase seek, a broad group of exploration has been produced in writing. Wang et al. [11] propose a positioned catchphrase inquiry plan which considers the importance scores of watchwords. Sadly, because of utilizing request safeguarding encryption (OPE) [12] to accomplish the positioning property, the proposed plan can't accomplish unlink ability of trapdoor. Later, Sun et al. [13] propose a multi-watchword content hunt plan which considers the importance scores of catchphrases and uses a multidimensional tree method to accomplish effective inquiry question. Yu et al. [14] propose a multi-watchword top-k recovery plan which utilizes completely Homomorphic encryption to encode the record/trapdoor and ensures high security. Cao et al. [6] propose a multi-watchword positioned look (MRSE), which applies direction machine as the catchphrase coordinating guideline, i.e., return information with the most coordinating catchphrases. Albeit numerous inquiry functionalities have been produced in past writing towards exact and proficient searchable encryption, it is still troublesome for searchable encryption to accomplish the same client experience as that of the plaintext pursuit, similar to Google look. This for the most part ascribes to taking after two issues. Firstly, inquiry with client inclinations is exceptionally main stream in the plaintext look [15], [16]. It empowers customized look and can all the more precisely speak to client's prerequisites, however has not been completely concentrated on and bolstered in the encoded information area. Furthermore, to further enhance the client's experience on looking, an imperative and major capacity is to empower the multi-watchword seek with the far reaching rationale operations, i.e., the "AND", "OR" and "NO" operations of catchphrases. This is central for inquiry clients to prune the looking space and rapidly distinguish the sought information. Cao et al. [6] propose the direction coordinating pursuit plan (MRSE) which can be viewed as a searchable encryption plan with "OR" operation. Zhang et al. [17] propose a conjunctive catchphrase pursuit plan which can be viewed as a searchable encryption plan with "AND" operation with the returned records coordinating all watchwords. On the other hand, most existing recommendations can just empower seek with single rationale operation, instead of the blend of numerous rationale operations on watchwords, which spurs our work. In this work, we address above two issues by creating two Fine-grained Multi-watchword Search (FMS) plans over encoded cloud information. Our unique commitments can be total margined in three angles as takes after:

•We present the pertinence scores and the inclination factors of watchwords for searchable encryption. The pertinence scores of watchwords can empower more exact returned results, and the inclination components of catchphrases speak to the significance of watchwords in the inquiry watchword set indicated via seek clients and correspondingly empowers customized hunt to take into account particular client inclinations. It in this manner further enhances the inquiry functionalities and client experience.

•We understand the "AND", "OR" and "NO" operations in the multi-catchphrase scan for searchable encryption. Com-pared with plans in [6], [13] and [14], the proposed plan can accomplish more far reaching usefulness and lower inquiry many-sided quality.

•We utilize the characterized sub-lexicons strategy to upgrade the effectiveness of the above two plans. Extensive tests exhibit that the improved plans can accomplish better proficiency as far as file building, trapdoor producing and inquiry in the examination with plans in [6], [13] and [14]. The rest of this paper is composed as takes after. In Section 2, we plot the framework model, danger model, security necessities and configuration objectives. In Section 3, we depict the preliminaries of the proposed plans. We show the created plans and improved plans in subtle elements in Section 4 and Section 5, separately. At that point we do the security investigation and execution assessment in Section 6 and Section 7, separately. Area 8 gives an

audit of the related works and Section 9 finishes up the paper.

2. SYSTEM MODEL, THREAT MODEL AND SECURITY REQUIREMENTS

2.1. System Model:

As appeared in Fig. 1, we consider a framework comprises of three substances.

•Data proprietor: The information proprietor outsources her information to the cloud for helpful and solid information access to the relating hunt clients. To ensure the information privacy-cy, the information proprietor encodes the first information through symmetric encryption. To enhance the pursuit efficient-cy, the information proprietor produces a few catchphrases for each outsourced archive. The relating record is then made by watchwords and a mystery key. After that, the information proprietor sends the encoded records and the relating files to the cloud, and sends the symmetric key and mystery key to inquiry clients.

•Cloud server: The cloud server is a middle of the road element which stores the scrambled archives and relates ing files that are gotten from the information proprietor, and gives information get to and pursuit administrations to inquiry clients. At the point when a pursuit client sends a watchword trapdoor to the cloud server, it would give back an accumulation of coordinating records in view of specific operations.

•Search client: An inquiry client inquiries the outsourced documents from the cloud server with taking after three stages. To start with, the hunt client gets both the mystery key and symmetric key from the information proprietor. Second, as indicated by the hunt watchwords, the pursuit client utilizes the mystery key to produce trapdoor and sends it to the cloud server. Last, she gets the coordinating archive gathering from the cloud server and unscrambles them with the symmetric key.

2.2. Threat Model and Security Requirements

In our threat model, the cloud server is assumed to be "honest-but-curious", which is the same as most related works on secure cloud data search [13], [14], [6]. Specifically, the cloud server honestly follows the designated protocol specification. However, the cloud server could be "curious" to infer and analyze data (including index) in its storage and message flows received during the protocol so as to learn additional information. we consider two threat models depending on the information available to the cloud server, which are also used in [13], [6].

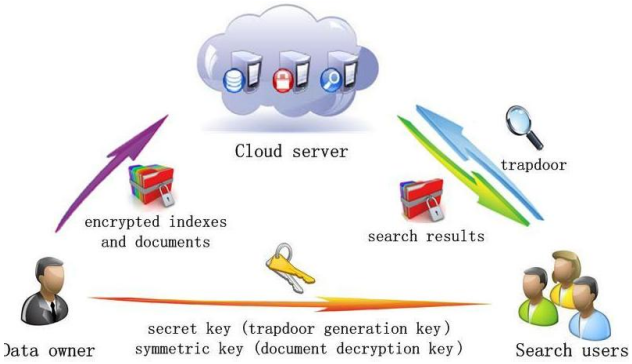


Fig 1. System Architecture

Known Ciphertext Model: The cloud server can just know scrambled archive gathering C and file accumulation I, which are both outsourced from the information proprietor.

•Known Background Model: The cloud server can have more learning than what can be gotten to in the known ciphertext model, for example, the connection relationship of trapdoors and the related factual of other data, i.e., the cloud server can have the measurable data from a known practically identical dataset which bears the comparable nature to the focusing on dataset.

Like [13], [6], we expect look clients are trusted elements, and they have the same symmetric key and mystery key. Seek clients have prior common trust with the information proprietor. For simplicity of representation, we don't consider the protected circulation of the symmetric key and the mystery key between the information proprietor and inquiry clients; it can be accomplished through consistent confirmation and secure channel foundation conventions in view of the former security setting shared between pursuit clients and the information proprietor [18]. What's more, to make our presentations more engaged, we don't consider after issues, including the entrance control issue on overseeing decoding abilities given to clients and the information gathering's upgrading issue on embeddings new records, overhauling existing archives, and erasing existing reports, are isolated issues. The intrigued perusers on above issues may

allude to [6], [5], [10], [19]. In view of the above danger model, we characterize the security necessities as takes after:

•Confidentiality of records: The outsourced reports gave by the information proprietor are put away in the cloud server. On the off chance that they coordinate the pursuit watchwords, they are sent to the inquiry client. Because of the security of reports, they ought not be identifiable with the exception of by the information proprietor and the approved pursuit clients.

•Privacy security of record and trapdoor: As examined in Section 2.1, the file and the trapdoor are made taking into account the archives' watchwords and the hunt catchphrases, separately. On the off chance that the cloud server recognizes the substance of file or trapdoor, and further finds any relationship in the middle of catchphrases and scrambled archives, it may take in the real subject of a record, even the substance of a short report [20]. In this way, the substance of file and trapdoor can't be distinguished by the cloud server.

•Unlink capacity of trapdoor: The reports put away in the cloud server may be sought ordinarily. The cloud server ought not have the capacity to realize any watchword data as indicated by the trapdoors, e.g., to decide two trapdoors which are begun from the same catchphrases. Something else, the cloud server can reason relationship of trapdoors, and debilitate to the protection of catchphrases. Henceforth the trapdoor era capacity ought to be randomized, as opposed to deterministic.

3. PROPOSED SCHEMES:

In cloud computing, secure analysis on outsourced encrypted data is a major topic. As a often used query for online applications, secure k-nearest neighbors (k-NN) computation on encrypted cloud data has inward much notice, and several solutions for it have been put forward. on the other hand, most existing schemes assume the query users are fully trusted and all query users share the total key which is used to encrypt and decrypt data holder's outsourced data. It is constitutionally not realistic in lots of real-world applications.

Here we propose a novel secure and efficient scheme for k-NN query on encrypted cloud data in which the key of data owner to encrypt and decrypt outsourced data will not be completely reveal to any query user. so, our scheme can efficiently support the secure k-NN query on encrypted cloud data even when query users are not reliable enough.

Secure scheme:

A model for Secure Computation on Encrypted Database (SCONEDB) Encrypted DBMS (EDBMS) hosting at an untrusted service provider to Store encrypted data Process queries. Let us take an example i.e Three Players Game „

Player 1 : **Database owner –** Encrypts data and send them to the Database at the service provider „

Player 2 : **User of the database –** They issue queries to the EDBMS „

Player 3 : **Attacker** – try to break in to the encrypted database.

Problem definition:

Define an encryption scheme (ET, EQ and D) and a query processing method on E(DB) such that query results returned are correct and the attacker cannot compromise the E(DB), i.e., DBA is empty, given background knowledge H.

Attack Model: Three levels of background knowledge

Basic capability: Attacker has full access to encrypted data „ Background knowledge (a three level model): „ Level 1 : no background knowledge „ Level 2 : attacker knows some records in DB (plain text) „ Level 3 : attacker knows some records in DB and the encrypted values of these records, i.e., knows some (x, E(x)) pairs.

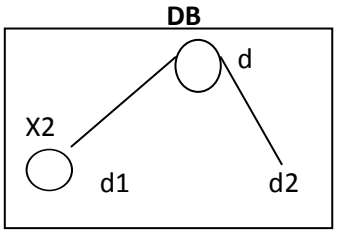
SCONEDB on an important query type: Secure kNN Computation:

We develop an encryption scheme for kNN queries on SECONEDB to explore its applicability.

„ k nearest neighbor query (kNN)

Database DB: a set of d dimensional points

Given a query point q, find the k nearest points to q in the database.



In the above figure it is clearly shown that x2 is the 1-nearest neighbor of q.

Nice property for kNN query on E(DB):

In fact, we only need to compute the "distance differential" from a query point. (Is x 2 closer to q than

x 1 ?)
| |x 1 – q| | – | |x 2 – q| | > 0 --------- (1)
⇔(x 1.x1 – 2x 1.q) – (x 2.x 2 – 2x 2.q) > 0
⇔((x 2, -0.5(x 2.x 2)) . (q, 1) <
((x 1, -0.5(x 1.x 1)) . (q, 1) ---------- (2)
⇔x 2*. q* < x 1*. q* ⇔E(x 2*).E (q*) <
E(x 1*).E(q*)----------(3)
where x* = (x, -0.5(x.x)) and q* = (q, 1)

Nice property: When q arrives, if we can compute x*.q* for different data points x in the encrypted data space, we can then determine which data point x is close to q.

4. PERFORMANCE EVALUATION:

Mainstream cryptography has its methodology and goal. Aim at the "most stringent" provable security.
Security goal (semantic security) „
i) Basic requirement: protect the plain text (data) against attack
ii) Additional requirement: protect any statistical information on the plain text (data) against attack „
e.g., more than half of the bank customers have 0.5M + in their accounts. Adversary power – strong attack model „ i) capability assumption: attacker can have an oracle to encrypt/decrypt plaintext/ciphertext „ e.g., Chosen Plaintext Attack (CPA), Chosen Ciphertext Attack (CCA) „
iii) Background knowledge assumption: attacker can obtain background knowledge h(x) on plain text x for any function h „ .e.g., know the relative frequencies of alphabets in English .Problem on computation – performance is often scarified.

5. CONCLUSION:

Our proposed schema defines that a novel secure and efficient scheme for k-NN query on encrypted cloud data in which the key of data owner to encrypt and decrypt outsourced data will not be completely reveal data to any query user. so, our scheme can efficiently support the secure k-NN query on encrypted cloud data even when query users are not reliable enough. Not only that the schema will protect any statistical information on the plain text (data) against attack.„

REFERENCES

[1] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, "An smdp-based service model for interdomain resource allocation in mobile cloud networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 5, pp. 2222–2232, 2012.

[2] M. M. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 1805–1818, 2012.

[3] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, "Exploiting geo-distributed clouds for e-health monitoring system with minimum service delay and privacy preservation," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, pp. 430–439, 2014.

[4] T. Jung, X. Mao, X. Li, S.-J. Tang, W. Gong, and L. Zhang, "Privacy-preserving data aggregation without secure channel: multivariate poly-nomial evaluation," in Proceedings of INFOCOM. IEEE, 2013, pp. 2634–2642.

[5] Y. Yang, H. Li, W. Liu, H. Yang, and M. Wen, "Secure dynamic searchable symmetric encryption with constant document update cost," in Proceedings of GLOBCOM. IEEE, 2014, to appear.

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.

[7] https://support.google.com/websearch/answer/173733?hl=en.

[8] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proceedings of S&P. IEEE, 2000, pp. 44–55.

[9] R. Li, Z. Xu, W. Kang, K. C. Yow, and C.-Z. Xu, "Efficient multi-keyword ranked query over encrypted data in cloud computing," Future Generation Computer Systems, vol. 30, pp. 179–190, 2014.

[10] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. Shen, "Enabling efficient multi-keyword ranked search over encrypted cloud data through blind storage," IEEE Transactions on Emerging Topics in Computing, 2014, DOI10.1109/TETC.2014.2371239.

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

