International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue:1 January 2017 p-ISSN: 2394-8280

A REVIEW ON SECURE AND DYNAMIC MULTI-KEYWORD RANKED SEARCH SCHEME OVER ENCRYPTED CLOUD DATA

Miss.Tejashree Ajit Rahane[1] , Prof.S.K.Sonkar[2]

[1]*Student,Department of Computer Engineering,Amrutvahini COE, Sangamner,Savitribai Phule Pune University,Pune India.*
tejashreerahane@gmail.com
[2]*Assistant Professor, Department of Computer Engineering,Amrutvahini COE, Sangamner,SavitribaiPhule Pune University, Pune India.*
sonkar83@gmail.com

Abstract

Now a days there will be growing popularity of cloud computing, large number of users and data owners are motivated to outsource their data to cloud servers for large convenience and reduced cost required for data management. However, important data should be encrypted before outsourcing for privacy requirements, which uses data utilization technique like keywordbased document recovery. A secure multi-keyword rankedsearch scheme over encrypted cloud data, which concurrently supports dynamic update operations like deletion and insertion of documents. Mostly, the vector space model and the widely used TF-IDF model are combined in the index construction and query generation. Creating a special tree-based index structure with the help of Greedy Depth-first Search algorithm which gives well organized multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and for the time being ensures accurate relevance score calculation between encrypted index and query vectors. Dummy terms are added to the index vector for blinding search results, in order to resist statistical attacks. Due to the use of special tree-based index structure, the proposed concept can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to express the efficiency of the proposed scheme.

Index Terms— Searchable encryption, multi-keyword ranked search, dynamic update, cloud computing

Literature Survey

Kui Ren, et.al [1] Distributed computing speaks to today's most energizing registering outlook change in data innovation. Be that as it may, security and protection are seen as essential deterrents to its wide reception. Here, the creator's plot a few basic security challenges and propel advance examination of security answers for a dependable open cloud environment. Distributed computing is the most up to date term for the since quite a while ago imagined vision of processing as a utility. The cloud gives helpful, on-request organize access to a brought together pool of configurable figuring assets that can be quickly sent with incredible productivity and negligible administration overhead.1 With its un-priority favorable circumstances, distributed computing empowers a basic outlook change by the way we convey and convey processing administrations that is, it makes conceivable registering outsourcing to such an extent

that both people and ventures can abstain from conferring substantial capital expenses when buying and overseeing programming and equipment, and additionally managing the operational overhead in that.

S. Kamara and K. Lauter[2] Motivated to the issue of building a safe distributed storage benefit on top of an open cloud framework where the specialist co-op is not totally trusted by the client. We portray, at an abnormal state, a few structures that consolidate later and non-standard cryptographic primitives keeping in mind the end goal to accomplish our objective. We study the advantages such a design would give to both clients and specialist co-ops and give a review of late advances in cryptography roused particularly by distributed storage.

C. Gentry[3] Discuss to propose the flrst completely homomorphic encryption conspire, taking care of a focal open issue in cryptography. Such a plan permits one to process subjective capacities over encoded information without the decoding key { i.e., given encryptions E(m1); E(mt) of m1; mt, one can effciently register a reduced ciphertext that scrambles f(m1;mt) for any effciently calculable capacity f. This issue was postured by Rivest et al. in 1978. Completely homomorphic encryption has various applications. For instance, it empowers private inquiries to an internet searcher { the client presents an encoded question and the web index registers a brief scrambled reply while never taking a gander at the inquiry free. It likewise empowers seeking on encoded information { a client stores scrambled flles on a remote flle server and can later have the server recover just flles that (when unscrambled) fulfill some boolean limitation, despite the fact that the server can't decode the flles all alone. All the more comprehensively, completely homomorphic encryption enhances the e–ciency of secure multiparty calculation. Our development starts with a fairly homomorphic \boostrappable" encryption conspire that works when the capacity f is the plan's own particular decoding capacity. We then show how, through recursive self-inserting, bootstrappable encryption gives completely homomorphic encryption. The onstruction makes utilization of difficult issues on perfect cross sections.

O. Goldreich and R. Ostrovsky [4] In this paper, we display a hypothetical treatment of programming assurance. Specifically, we distil and plan the key issue of finding out about a program from its execution, and diminish this issue to the issue of on-line reproduction of a subjective program on a careless RAM. We then present our principle result: a productive reproduction of a self-assertive (RAM) program on a probabilistic unmindful RAM. Expecting that restricted capacities exists, we demonstrate how one can make our product security conspire hearty against a polynomial-time foe who is permitted to adjust memory substance amid execution in a dynamic mold. We start by examining programming assurance.

D. Bonehet.al [5]: Motivate to concentrate the issue of looking on information that is scrambled utilizing an open key framework. Consider client Bob who sends email to client Alice encoded under Alice's open key. An email portal needs to test whether the email contains the catchphrase \urgent" so it could course the email appropriately. Alice, then again does not wish to give the passage the capacity to decode every one of her messages. We characterize and develop an instrument that empowers Alice to give a key to the entryway that empowers the portal to test whether the word \urgent" is a watchword in the email without learning whatever else about the email. We allude to this system as Public Key Encryption with catchphrase Search. As another case, consider a mail server that stores different messages freely scrambled for Alice by others. Utilizing our component Alice can send the mail server a key that will empower the server to recognize all messages containing some particular catchphrase, yet learn nothing

else. We characterize the idea of open key encryption with watchword pursuit and give a few developments.

D. X. Song et.al [6]: It is alluring to store data on data stockpiling servers, for instance, mail servers and record servers fit as a fiddle to reduce security and assurance threats. Regardless, this when in doubt proposes that one needs to surrender value for security? For example, if a client wishes to recuperate just records containing certain words, it was not previously known how to let the data stockpiling server play out the interest and answer the question without loss of data mystery. In this paper, we delineate our cryptographic arrangements for the issue of looking for on mixed data and give affirmations of security to the consequent crypto systems. Our techniques have different basic purposes of intrigue. They are provably secure: they give provable puzzle to encryption, as in the untrusted server can't learn anything about the plaintext when simply given the ciphertext; they give request constrainment to wanders, suggesting that the untrusted server can't learn much else about the plaintext than the inquiry thing; they give controlled looking for, so that the untrusted server can't search for an optional word without the customer's endorsement; they in like manner reinforce covered inquiries, so that the customer may approach the untrusted server to filter for a secret word without revealing the word to the server. The computations we present are essential, brisk (for a record of length n, the encryption and chase estimations simply require O(n) stream figure and piece figure operations), and present no space and correspondence overhead, and from this time forward are helpful to use today.

Y.-C. Chang and M. Mitzenmacher [7] Discuss consider the accompanying issue: a client U needs to store his records in a scrambled frame on a remote document server S. Later the client U needs to effectively recover a portion of the encoded records containing (or listed by) particular catchphrases, keeping the watchwords themselves mystery and not imperiling the security of the remotely put away documents. For instance, a client might need to store old email messages encoded on a server oversaw by Yahoo or another vast merchant, and later recover certain messages while going with a cell phone. In this paper, we offer answers for this issue under all around characterized security necessities. Our plans are proficient as in no open key cryptosystem is included. Without a doubt, our approach is autonomous of the encryption strategy decided for the remote records. They are likewise incremental, in that U can submit new documents which are absolutely secure against past inquiries yet at the same time searchable against future questions.

R. Curtmola et.al [8]: Searchable symmetric encryption (SSE) permits a gathering to outsource the capacity of his information to another gathering in a private way, while keeping up the capacity to specifically seek over it. This issue has been the concentration of dynamic research and a few security definitions and developments have been proposed. In this paper we start by looking into existing ideas of security and propose new and more grounded security definitions. We then present two developments that we indicate secure under our new definitions. Strangely, notwithstanding fulfilling more grounded security ensures, our developments are more productive than every single past development. Further, earlier work on SSE just considered the setting where just the proprietor of the information is equipped for submitting seek questions. We consider the regular augmentation where a subjective gathering of gatherings other than the proprietor can submit seek questions. We formally characterize SSE in this multi-client setting, and present a proficient development.

CONCLUSION

All of the existing System having how to secure search encrypted data from cloud System.a secure, efficient and dynamic search scheme is proposed, which supports not only the accurate multi-keyword ranked search but also the dynamic deletion and insertion of documents. We construct a special keyword balanced binary tree as the index, and propose a "Greedy Depth-first Search" algorithm to obtain better efficiency than linear search. In addition, the parallel search process can be carried out to further reduce the time cost. The security of the scheme isprotected against two threat models by using the secure kNN algorithm. Experimental results demonstrate the efficiency of our proposed scheme. There are still many challenge problems in symmetric SE schemes. In the proposed scheme, the data owner is responsible for generating updating information and sending them to the cloud server. Thus, the data owner needs to store the unencrypted index tree and the information that are necessary to recalculate the IDF values. Such an active data owner may not be very suitable for the cloud computing model. It could be a meaningful but difficult future work to design a dynamic searchable encryption scheme whose updating operation can be completed by cloud server only, meanwhile reserving the ability to support multi-keyword ranked search. In addition, as the most of works about searchable encryption, our scheme mainly considers the challenge from the cloud server.

References:

[1] K. Ren, C. Wang, Q. Wang et al., "Security challenges for the public cloud," IEEE Internet Computing,vol. 16, no. 1, pp. 69–73, 2012.
[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security.Springer,2010,pp.136–149.
[3] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.
[4] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," Journal of ACM(JACM),vol.43,no.3,pp.431–473,1996.
[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in CryptologyEurocrypt 2004. Springer, 2004, pp. 506–522.
[6] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pirqueries,"inAdvances in
Cryptology-CRYPTO 2007. Springer, 2007, pp. 50–67.
[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P
2000.Proceedings.2000 IEEE Symposiumon.IEEE, 2000, pp. 44– 55.
[8] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.
[9] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proceedings of the Third international conference on Applied Cryptography and Network Security. Springer-Verlag, 2005, pp. 442–455.
[10] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88