International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

A Secure and Dynamic Keyword Ranked Search Scheme over Encrypted Cloud Data Using Abe

G.Renuka & P.R.Rajesh Kumar
[1]M.Tech Student, Dept. of CSE, SKU College of Engineering, Anantapur, India.
[2]Lecturer,Dept. of CSE, SKU College of Engineering, Anantapur, India.

ABSTRACT:

Perceptive information ought to be encrypted before outsourcing for privacy wants, which obsoletes information utilization like keyword-based document retrieval. Cloud computing has become more and {more} more fashionable for information homeowners to source their information to public cloud servers whereas permitting information users to retrieve this information. For privacy issues, secure searches over encrypted cloud information have intended many analysis works underneath the one owner model. We are able to secure multi-keyword hierarchal search theme over encrypted cloud information, which at the same time supports dynamic update operations like deletion and insertion of documents. During this paper, we have a tendency to propose schemes to traumatize Privacy protective hierarchal Multi-keyword Search in an exceedingly Multi-owner model (PRMSM). To modify cloud servers to perform secure search while not knowing the particular information of each keywords and trapdoors, we have a tendency to consistently construct a unique secure search protocol. To rank the search results and preserve the privacy of relevance's scores between keywords and files, we have a tendency to propose a unique Additive Order and Privacy protective perform family. What is more, PRMSM supports economical information user revocation. In depth experiments on real-world datasets ensure the efficaciousness and potency of PRMSM.

KEYWORDS: Multi-keyword ranked search over encrypted cloud data, Product resemblance, Cloud, Data owners

INTRODUCTION:

Now a day's cloud computing has become essential for several utilities, wherever cloud customers will slightly store their information into the cloud thus on enjoy on-demand high quality request and services from a shared pool of configurable computing resources. Its large suppleness and monetary savings area unit attracting each persons and enterprise to source their native complicated information management system into the cloud. On the one hand, to congregate the economical information retrieval demand, the large quantity of documents orders the cloud server to realize result connection ranking, as another of returning undifferentiated results. Such graded search system permits information users to find the foremost acceptable data quickly, instead of burdensomely sorting throughout each match within the content cluster. Graded search can even graciously take away redundant network traffic by transferring the foremost relevant information, which is extremely engaging within the "pay-as-you-use" cloud thought. For privacy protection, such ranking operation on the opposite hand shouldn't reveal any keyword to connected data. to induce higher the search result exactitude moreover on improve the user looking out expertise, it's additionally essential for such ranking system to support multiple keywords search, as single keyword search typically hand over way too common results. As a daily follow specifies by today's internet search engines i.e. Google search, information users might lean to supply a group of keywords as another of only 1 because the indicator of their search interest to retrieve the foremost relevant information. And every keyword within the search demand is in a position to assist slender down the search result more.

LITERATURE SURVEY:

1) A view of cloud computing, "M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia", Cloud computing, the long-held dream of computing as a utility, has the potential to rework an oversized a part of the IT business, creating code even a lot of engaging as a service and shaping the method IT hardware is intended and purchased. Developers with innovative concepts for brand spanking new net services not need the massive capital outlays in hardware to deploy their service or the human expense to control it. they have not worry concerning over provisioning for a service whose quality doesn't meet their predictions, therefore wasting pricey resources, or under provisioning for one that becomes wildly in style, therefore missing potential customers and revenue. Moreover, firms with massive batch-oriented tasks will get results as quickly as their programs will scale. This snap of resources, while not paying a premium for giant scale, is new within the history of IT.

2) Privacy preserving public auditing for secure cloud storage, "C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou",

Using cloud storage, users will remotely store their knowledge and luxuriate in the on-demand high-quality applications and services from a shared pool of configurable computing resources, while not the burden of native knowledge storage and maintenance. However, the actual fact that user now not has physical possession of the outsourced knowledge makes the information integrity protection in cloud computing a formidable task, particularly for users with forced computing resources. Moreover, users ought to be ready to simply use the cloud storage as if it's native, without fear regarding the requirement to verify its integrity. Thus, sanctioning public auditability for cloud storage is of important importance so users will resort to a third-party auditor (TPA) to examine the integrity of outsourced knowledge and be worry free. To firmly introduce a good TPA, the auditing method ought to usher in no new vulnerabilities toward user knowledge privacy, and introduce no extra on-line burden to user. During this paper, we have a tendency to propose a secure cloud storage system supporting privacy-preserving public auditing. We have a tendency to more extend our result to modify the TPA to perform audits for multiple users at the same time and with efficiency. In depth security and performance analysis show the projected schemes square measure demonstrably secure and extremely economical. Our preliminary experiment conducted on Amazon EC2 instance more demonstrates the quick performance of the look.

3) Practical techniques for searches on encrypted data, " D.Song, D.Wagner, and A.Perrig", It is fascinating to store knowledge on knowledge storage servers like mail servers and file servers in encrypted kind to cut back security and privacy risks. However this sometimes implies that one needs to sacrifice practicality for security. As an example, if a shopper needs to retrieve solely documents containing sure words, it had been not antecedently famous a way to let the information storage server perform the search and answer the question, while not loss of knowledge confidentiality. We have a tendency to describe our scientific discipline schemes for the matter of looking on encrypted knowledge and supply proofs of security for the ensuing crypto systems. Our techniques have variety of crucial blessings. they're incontrovertibly secure: they supply obvious secrecy for encoding, within the sense that the un trusted server cannot learn something regarding the plaintext once solely given the cipher text; they supply question isolation for searches, which means that the un trusted server cannot learn something additional regarding the plaintext than the search result; they supply controlled looking, so the un trusted server cannot look for associate arbitrary word while not the user's authorization; they additionally support hidden queries, so the user could raise the un trusted server to look for a secret word while not revealing the word to the server. The algorithms bestowed area unit easy, quick (for a document of length n, the encoding and search algorithms solely want O(n) stream cipher and block cipher operations), and introduce nearly no house and communication overhead, and thus area unit sensible to use nowadays

4) Searchable symmetric encryption: improved definitions and efficient constructions, "R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky", Searchable radial coding (SSE) permits a celebration to source the storage of its information to a different party (a server) in a very personal manner, whereas maintaining the flexibility to by selection search over it. This drawback has been the main target of active analysis in recent years. During this paper we have a tendency to show 2 solutions to compass point that at the same time relish the subsequent properties: Both solutions square measure additional economical than all previous constant-round schemes. Particularly, the work performed by the server per came back document is constant as against linear within the size of the information. Each solutions relish stronger security guarantees than previous constant-round schemes. In fact, we have a tendency to show delicate however serious issues with previous notions of security for compass point, and show a way to style constructions that avoid these pitfalls. Further, our second resolution conjointly achieves what we have a tendency to decision reconciling compass point security, wherever queries to the server are often chosen adaptively (by the adversary) throughout the execution of the search; this notion is each necessary in apply and has not been antecedently thought of. Amazingly, despite being safer and additional economical, our compass point schemes square measure remarkably straightforward. We have a tendency to take into account the simplicity of each solution as a very important step towards the readying of compass point technologies as an extra contribution; we have a tendency to conjointly take into account multi-user compass point. All previous work on compass point studied the setting wherever solely the owner of the information is capable of submitting search queries. We have a tendency to take into account the natural extension wherever associate degree discretional cluster of parties apart from the owner will submit search queries. We have a tendency to formally outline compass point within the multi-user setting, associate degreed gift an economical construction that achieves higher performance than merely exploitation access management mechanisms.

5) Public key encryption with keyword search secure against keyword guessing attacks without random oracle, " D. B. et al",

The notion of public key coding with keyword search (PEKS) was place forth by Boneh et al. to modify a server to go looking from a set of encrypted emails given a "trapdoor" (i.e., associate encrypted keyword) provided by the receiver. The great property during this theme permits the server to go looking for a keyword, given the trapdoor. Hence, the supporter will simply use associate un trusted server, which makes this notion terribly sensible. Following Boneh et al.'s work, there are succeeding works that are planned to boost this notion. 2 necessary notions embody the questionable keyword estimation attack and secure channel free, planned by Byun et al. and Baek et al., severally. The previous realizes the very fact that in apply; the area of the keywords used is incredibly restricted, whereas the latter considers the removal of secure channel between the receiver and therefore the server to create PEKS sensible. Sadly, the prevailing construction of PEKS secure against keyword estimation attack is simply secure below the random oracle model, that doesn't replicate its security within the planet. Moreover, there's no complete definition that captures secure channel free PEKS schemes that area unit secure against chosen keyword attack, chosen cipher text attack, and against keyword estimation attacks, despite the fact that these notions appear to be the foremost employment of PEKS primitives. During this paper, we tend to build the subsequent contributions. First, we tend to outline the strongest model of PEKS that is secure channel free and secure against chosen keyword attack, chosen cipher text attack, and keyword estimation attack. Specially, we tend to gift 2 necessary security notions particularly IND-SCF-CKCA and IND-KGA. The previous is to capture an internal someone, whereas the latter is to capture an outdoor someone. Intuitively, it ought to be clear that IND-SCF-CKCA captures a additional rigorous attack compared to IND-KGA. Second, we tend to gift a secure channel free PEKS theme secure while not random oracle below the renowned assumptions, namely DLP, DBDH, SXDH and truncated q-ABDHE assumption. Our contributions fill the gap within the literature and thence, creating the notion of PEKS terribly sensible. We tend to shall highlight that our theme is IND-SCF-CKCA secure.

RELATED WORK:

Existing System:

Secure search over encrypted knowledge has recently attracted the interest of the many researchers. Song et al. initial outline and solve the matter of secure search over encrypted knowledge. They propose the conception of searchable encoding, which may be a science primitive that allows users to perform a keyword-based search on associate encrypted dataset, even as on a plaintext dataset. Searchable encoding is more developed.

Secure search over encrypted cloud knowledge is initially outlined by Wang et al. and more developed. These researches not solely scale back the computation and storage value for secure keyword search over encrypted cloud knowledge, however conjointly enrich the class of search operate, together with secure stratified multi-keyword search, fuzzy keyword search, and similarity search.

DISADVANTAGES OF EXISTING SYSTEM:

Existing schemes area unit involved largely with single or mathematician keyword search.

The entire present schemes area unit restricted to the single-owner model. As a matter of reality, most cloud servers in apply don't simply serve one knowledge owner; instead, they usually support multiple knowledge house owners to share the advantages brought by cloud computing.

PROPOSED SYSTEM:

In this paper, we have a tendency to propose PRMSM, a privacy conserving stratified multi-keyword search protocol during a multi-owner cloud model.

We outline a multi-owner model for privacy conserving keyword search over encrypted cloud knowledge.

We propose associate economical knowledge user authentication protocol, that not solely prevents attackers from eavesdropping secret keys and deceit to be miser knowledge users activity searches, however conjointly allows knowledge user authentication and revocation.

We consistently construct a unique secure search protocol, that not solely allows the cloud server to perform secure stratified keyword search while not knowing the particular knowledge of each keywords and trapdoors, however conjointly permits knowledge house owners to encipher keywords with self-chosen keys and permits documented knowledge users to question while not knowing these keys.

We propose associate Additive Order and Privacy conserving operate family (AOPPF) that permits knowledge house owners to shield the privacy of connation scores exploitation totally different functions consistent with their preference, whereas still allowing the cloud server to rank the info files accurately.

We conduct in depth experiments on real-world datasets to verify the efficaciousness and potency of our planned schemes.

ADVANTAGES OF PROPOSED SYSTEM:

The planned theme permits multi-keyword search over encrypted files which might be encrypted with totally different keys for various knowledge house owners.

The planned theme permits new knowledge owners to enter this method while not moving different knowledge owners or knowledge users, i.e., the theme supports knowledge owner measurability during a plug-and-play model.

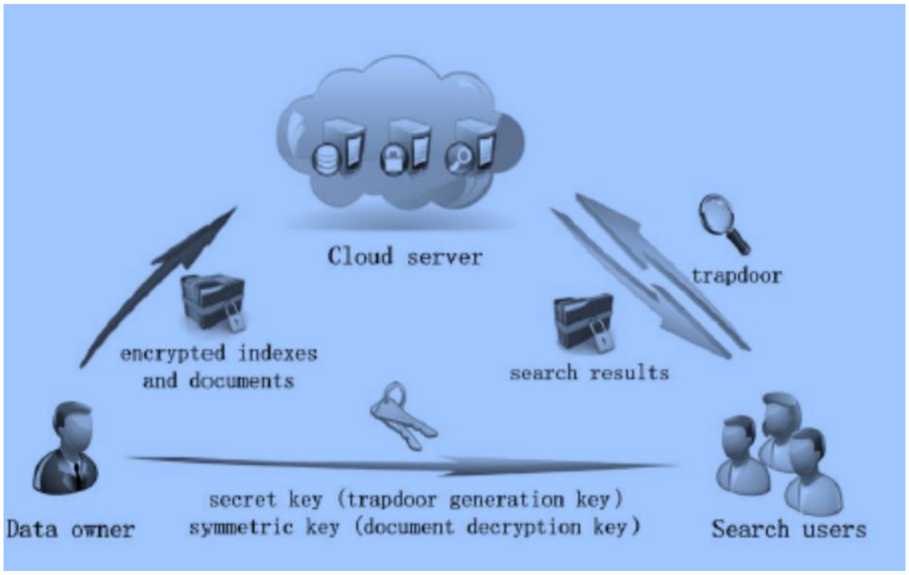
The planned theme ensures that solely documented knowledge users will perform correct searches. Moreover, once a knowledge user is revoked, he will not perform correct searches over the encrypted cloud knowledge.

To modify cloud servers to perform secure search while not knowing the particular price of each keywords and trapdoors, we have a tendency to consistently construct a unique secure search protocol. As a result, completely different knowledge house owners use different keys to encipher their files and keywords. Documented knowledge users will issue a question while not knowing secret keys of those totally different knowledge house owners.

To rank the search results and preserve the privacy of connation scores between keywords and files, we have a tendency to propose a brand new additive order and privacy conserving operate family, which helps the cloud server come the foremost relevant search results to knowledge users while not revealing any sensitive data.

To stop the attackers from eavesdropping secret keys and deceit to be legal knowledge users submitting searches, we have a tendency to propose a unique dynamic secret key generation protocol and a brand new knowledge user authentication protocol.

SYSTEM ARCHITECTURE:



IMPLEMENTATION:

MODULES:

System Model

Data User Authentication

Illegal Search Detection

Search over Multi-owner

MODULES DESCRIPTION:

System Model

In the primary module, we tend to develop the System Model to implement our planned system. Our System model consists of Admin, users, information house owners, and Cloud Servers. Admin provides the accessibility to Data-owners. at first Data-owner must register and admin approves the every information owner request. The individual watchword and login credentials are going to be sent to the e-mail ID of knowledge owner.

In Users sub-module, every user includes a world identity within the system. A user is also entitled a group of attributes which can return from multiple attribute authorities. The user can receive a secret key related to its attributes entitled by the corresponding attribute authorities.

In information house owners sub-module, the planned theme ought to permit new information owners to enter this method while not moving different information owners or information users, i.e., the theme ought to support information owner measurability in an exceedingly plug-and-play model.

In Cloud Server sub-module of system model, the owner sends the encrypted information to the cloud server through Admin. They are doing not consider the server to try and do information access management. But, the access management happens within the cryptography. That's only the user's attributes satisfy the access policy outlined within the cipher text; the user is ready to decode the cipher text. Thus, users with totally different attributes will decode different range of content keys and so acquire different granularities of knowledge from a similar data.

Data User Authentication

To forestall attackers from dissembling to be legal information users acting searches and launching applied math attacks supported the search result, information users should be echo before the administration server re-encrypts trapdoors for information users. Ancient authentication ways typically follow 3 steps. First, information requester and information appraiser share a secret key, say, k0. Second, the requester encrypts his in person recognizable info d0 victimization k0 and sends the encrypted information (d0)k0 to the appraiser. Third, the appraiser decrypts the received information with k0 and authenticates the decrypted information.

The key purpose of a prospering authentication is to produce each the dynamically ever-changing secret keys and therefore the historical information of the corresponding information user.

Illegal Search Detection

In our theme, the authentication method is protected by the dynamic secret key and therefore the historical info. We tend to assume that Associate in nursing assaulter has with success eaves dropped the key. Then he must construct the authentication information; if the assaulter has not with success eaves dropped the historical data, e.g., the request counter, the last request time, he cannot construct the right authentication information. So this amerceable action can before long be detected by the administration server.

Further, if the assaulter has with success eavesdropped all information of Uj , the assaulter will properly construct the authentication information and fake himself to be Uj while not being detected by the administration server. However, once the legal information user Uj performs his search, since the key on the administration server aspect has modified, there'll be contradictory secret keys between the administration server and therefore the legal information user. Therefore, the info user and administration server can before long observe this amerceable action.

Search over Multi-owner:

The planned theme ought to permit multi-keyword search over encrypted files which might be encrypted with totally different keys for various information house owners. It conjointly must permit the cloud server to rank the search results among totally different information house owners and come back the top-k results. The cloud server stores all encrypted files and keywords of various information house owners.

The administration server also will store secret information on the cloud server. Upon receiving a question request, the cloud can search over the information of these data house owners. The cloud processes the search request in 2 steps. First, the cloud matches the queried keywords from all keywords hold on thereon, and it gets a candidate file set. Second, the cloud ranks files within the candidate file set and finds the foremost top-k relevant files. Finally, we tend to apply the planned theme to encipher the connation scores and acquire the top-k search results.

CONCLUSION:

To alter the cloud server to perform secure search among multiple owners' information encrypted with totally different secret keys, we tend to consistently construct a unique secure search protocol. To with efficiency certify information users and establish attackers World Health Organization steal the key and perform amerceable searches, we tend to propose a unique dynamic secret key generation protocol and a brand new information user authentication protocol. During this analysis paper, we tend to investigate the matter of secure multi-keyword look for multiple information house owners and multiple information users within the cloud computing surroundings. Uncommon from previous works, our schemes alter approved information users to get secure, convenient, and economical searches over multiple information owners' information. We tend to propose a unique Additive Order and Privacy protective perform family. Moreover, we tend to show that our approach is computationally economical, even for big information and keyword sets. As our future work, reach the perfect state due to the keyword weight. We are going to develop some way to mirror the keyword weight and alter update and multi information owner theme has additional realistic significance.

REFERENCES:

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Communication of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.

[3] D.Song, D.Wagner, and A.Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE International Symposium on Security and Privacy (S&P'00)*, Nagoya, Japan, Jan. 2000, pp. 44–55.

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proc. ACM CCS'06*, VA, USA, Oct. 2006, pp. 79–88.

[5] D. B. et al., "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *EUROCRYPT*, vol. 43, pp. 506–522, 2004.

[6] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in *Proc. Applied Cryptography and Network Security (ACNS'04)*, Yellow Mountain, China, Jun. 2004, pp. 31–45.

[7] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in *Proc. IEEE Distributed Computing Systems (ICDCS'10)*, Genoa, Italy, Jun. 2010, pp. 253–262.

[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," in *Proc. IEEE INFOCOM'11*, Shanghai, China, Apr. 2011, pp. 829–837.

[9] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," *Parallel and Distributed Systems, IEEE*

Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[10] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 11, pp. 3025–3035, 2014.

[11] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient multikeyword ranked query on encrypted data in the cloud," in *Proc. IEEE Parallel and Distributed Systems (ICPADS'12)*, Singapore, Dec. 2012, pp. 244–251.

[12] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proc. IEEE INFOCOM'10*, San Diego, CA, Mar. 2010, pp. 1–5.

1. G.RENUKA has received the B. Tech (Information Technology) degree from IIT ATP college of engineering, Anantapur district (A.P) in 2014, and pursuing M. Tech(Computer science and Engineering) in Sri krishna Devaraya University College of Engineering and Technology., Anantapuramu district (AP).

P.R.RAJESH KUMAR received his B.Tech (Computer Scince and Engineering) Degree in from GATES, Anantapur, India, in 2005; M. Tech(Software Engineering) in JNTU, Anantapur,India, in 2012. he has experience of 10 years in teaching graduate level and she presently working as Lecturer in Department of CSE Sri krishnaDevaraya University College of Engineering. Anantapuramu district (AP).