PRIVACY-PRESERVING MULTI-KEYWORD TOP-K SIMILARITY SEARCH OVER ENCRYPTED DATA

Asst.pro Selvanayagi A, Deepak S, Diwakar T, Mohankumar G
Department of Computer Science and Engineering
M.Kumarasamy college of engineering
Karur

Abstract*—Countless proprietors has moved our information into cloud servers. Cloud information proprietors like to outsource records in an encoded frame for the capacity of secrecy protecting. Accordingly it is fundamental to create effective and solid figure content pursuit technique. One test is that the association between reports will be commonly shrouded in the methodology of encryption, which will provoke huge interest precision execution debasement. All entrance the in order from cloud by utilize the catchword based inquiry. The safe multi-catchphrase positioned seek from the encoded information from the cloud, top-k look issue for huge information encryption against protection ruptures, and endeavor to recognize a proficient and secure answer for this issue. It open operations like refresh, erase, and inclusion of archives. Here utilizing tree structure and shapeless scan technique for recover the information from the cloud. These sorts of procedures are utilized to tackle the issue of catchphrase speculating assault. The blowfish calculation for the encryption process. We propose a gathering multi-watchword top-k look conspire in view of parcel, where a gathering of tree-based records are developed for all documents. We join these strategies together into a proficient and secure way to deal with address our proposed top-k comparability seek here to decrease factual assaults. The broad test comes about on genuine informational indexes show that our approach can essentially enhance the capacity of guarding the protection breaks, the adaptability and the time productivity of inquiry handling over the cutting edge strategies. It can fulfill sub-coordinate interest time and the yield like different record recuperation furthermore oversee deletion and consideration of reports adaptably*

Keywords—*multi key search, data efficiency, secure data, blow fish, k-gram.*

I. INTRODUCTION

Cloud computing framework is a promising new innovation and incredibly quickens the advancement of extensive scale information stockpiling, handling and dispersion. In any case, security and protection wind up noticeably real concerns when information proprietors outsource their private information onto open cloud servers that are not inside their put stock in administration areas. To maintain a strategic distance from data spillage, delicate information must be encoded before transferring onto the cloud servers, which makes it a major test to help proficient catchphrase based questions and rank the coordinating outcomes on the scrambled information. Most present works just consider single watchword inquiries without proper positioning plans. In the ebb and flow multi-watchword positioned seek approach, the catchphrase lexicon is static and can't be broadened effortlessly when the quantity of watchwords increments. Besides, it doesn't consider the client conduct and watchword get to recurrence. For the question coordinating outcome which contains countless, the out-of-arrange positioning issue may happen. This makes it hard for the information buyer to discover the subset that is in all probability fulfilling its prerequisites. In this paper, we propose an adaptable multi-watchword question conspire, called MKQE to address the previously mentioned downsides. MKQE extraordinarily diminishes the upkeep overhead amid the catchphrase lexicon extension. It takes catchphrase weights and client get to history into thought while producing the inquiry result. Thusly, the archives that have higher access frequencies and that match nearer to the clients' entrance history get higher rankings in the coordinating outcome set. Our examinations demonstrate that MKQE presents better execution over the flow solutions. The watchword based information recuperation, which are extensively, used on the plaintext data than the interest from cloud server. A regular way to deal with diminish information spillage is data encryption. Be that as it may, this will influence server-to side information usage, for example, looking on scrambled information, turn into an extremely difficult errand. In the current years, analysts have proposed many figure content inquiry plots by fusing the cryptography systems. These techniques require enormous operations and have high time unpredictability.

In this framework have parcel of security issues are there Keyword Guessing Attack will happened the programmers can without much of a stretch figure the catchphrase than they can undoubtedly hack our substance from cloud server. Existing pursuit framework will give the outcome just in view of the Boolean catchphrase coordinating framework, it implies climate it will discover the precisely record name same as the watchword than the document will recovered from the server, it won't give any query output to incorrectly spelled watchwords. And furthermore the current pursuit framework never gives the outcome in view of comparable keyword. The able hunt plan to look through the archives from the cloud server utilizing multi-catchphrase. Here we utilizing the undefined catchphrase set it will make the all plausible incorrectly spell watchwords.Pursuit catchphrase get encode and it will check with the accumulation of unique scrambled the document name in the cloud server if the watchword will get coordinated then we interface the shapeless catchphrase set for that specific catchphrase and it look through the record list in view of that indistinct catchphrases, it will

recover the records from the cloud server and here we consider the seeking execution moreover. Broad trial comes about on genuine informational indexes exhibit that our proposed approach can altogether enhance the capacity of safeguarding the security ruptures, the adaptability and the time proficiency of inquiry preparing over the cutting edge strategies.

II. RELATED WORKS

1. Dawn Xiaodong Song, David Wagner, Adrian Perrig in 2015. Sensible Techniques for Searches on Encrypted Data. We depict our cryptographic plans for the issue of searching for on blended information and give affirmations of security to the subsequent crypto structures. Our strategies have different essential purposes of intrigue. They are provably secure: they give provable puzzle to encryption, as in the unfrosted server can't get anything about the plaintext when just given the figure content; they give question repression to looks, suggesting that the unfrosted server can't get the hang of much else about the plaintext than the inquiry thing; they give controlled seeking, so that the unfrosted server can't examine for a subjective word without the customer's endorsement; they moreover reinforce covered request, so the customer may approach the unfrosted server to search for a secret word without revealing the word to the server. The figuring's we display are essential, brisk (for a chronicle of length n, the encryption and chase counts simply require O(n) stream figure and square figure operations), and present no space and correspondence overhead, and therefore are even minded to use today. They are provably secure; they reinforce controlled and covered request and question repression. Direct and fast (More especially, for a report of length n, the encryption and request figuring's simply require O(n) stream figure and square figure operations).To exhibit no space and correspondence overhead. Our arrangement is also astoundingly versatile, and it can without quite a bit of extend be come to help additionally created request. We reason this gives an extreme new building discourage for the advancement of secure organizations in the untrusted establishment. The basic issue is that moving the estimation to the data amassing has all the earmarks of being to a great degree troublesome when the data is mixed. Looking for on encoded data using multi-party computation, yet it would require a high overhead, for example different servers. Particularly strong information theoretic security limits, which makes it harder to find realistic plans. Exhaust a ton of transmission limit, don't guarantee the characterization of the data, don't reinforce private watchword looking, and don't support controlled chasing or question separation.

2. Ning Cao, Cong Wang, Ming Li, KuiRen, Wenjing Lou in 2014Security Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data. This structure first time, we describe and handle the testing issue of insurance preservingmulti-watchword situated investigate encoded data in dispersed figuring (MRSE). We develop a course of action of strict security requirements for such a protected cloud data use structure. Among different multi-watchword semantics, we pick the fruitful similarity measure of "sort out arranging,"i.e., however many matches as could sensibly be normal, to get the essentialness of data records to the request question. We additionally use "internal thing likeness" to quantitatively evaluate such similarity measure. We at first propose a basic idea for the Rebased on secure internal thing computation, and after that give two on a very basic level upgraded MRSE intends to achieve distinctive stringent protection requirements in two assorted hazard models. To improve look comprehension of the data look for advantage, we encourage stretch out these two intends to help more interest semantics. Thorough examination investigating security and capability guarantees of proposed plans is given. Examinations on this present reality enlightening file also show proposed plans doubtlessly introduce low overhead on computation and communication.Multi-catchphrase situated looks for over mixed cloud data, and set up a variety of assurance necessities. These present reality instructive accumulations show our proposed plans exhibit low overhead on both figuring and communication. Without giving the ability to take a gander at secured internal things, predicate encryption isn't possessed all the necessary qualities for performing situated search. Such inefficiency load in like manner limits their judicious execution when sent in the cloud.

3. Zhihua Xia, Xinhui Wang, Xingming Sun, Qian Wang in 2013. A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data. We demonstrate a guaranteed multi-watchword arranged search for plot over encoded cloud information, which meanwhile underpins dynamic empower tasks like cancelation and thought of reports. Specifically, the vector space show up and the generally used TF _ IDF demonstrate are appreciated the record movement and request age. We develop a wonderful tree-based once-over structure and propose a "Voracious Depth-first Search" estimation to give proficient multi-catchphrase arranged look. The safe KNN computation is utilized to encode the document and request vectors, and in the meantime ensure exact congruity score estimation between mixed record and question vectors. Recalling a definitive target to confine obvious strikes, ghost terms are added to the record vector for blinding requested records. Because of the utilization of our remarkable tree-based summary structure, the proposed plan can achieve sub-straight chase time and deal with the cancelation and consideration of chronicles adaptably. Broad examinations are led to show the productivity of the proposed plot. A sheltered, viable and dynamic interest plot is proposed, which reinforces the exact multikeyword situated look for and additionally the dynamic eradication and option of records. The parallel interest process should be possible to moreover diminish the time cost. Troublesome future work to diagram a dynamic available encryption plot whose refreshing operation can be done by cloud server just, in the meantime saving the ability to help multi-catchphrase rankedsearch. It isn't practical and a dishonest data customer will incite many secure issues.

4. Wen Ming Liu, Lingyu Wang, Pengsu Cheng, KuiRen, Shunzhi Zhu and MouradDebbab in 2012PTP: Privacy-Preserving Traffic Padding in Web-Based Application. We at first watch a fascinating closeness between this security sparing action padding (PPTP) issue and anotherall-around considered issue, assurance defending data distributing (PPDP). In light of such a similarity, we demonstrate a formal PPTPmodel wrapping the assurance requirements, padding costs, and padding methods. We by then detail PPTP issues under various application circumstances, separate their multifaceted nature, and layout capable heuristic figuring's. Finally, we attest the adequacy and viability of our computations by standing out them from existing courses of action through tests using certifiable Web applications. Demonstrated a captivating relationship between the movement padding issue of Web applications and the security preservingdata circulating. Our investigations with genuine applications have avowed the execution of our responses for be superior to existing ones to the extent correspondence and figuring overhead.\

5. Jin Li, Qian Wang, Cong Wang, Ning Cao, KuiRen, and Wenjing Lou in 2011. Fluffy Keyword Search over Encrypted Data in Cloud Computing. As Cloud Computing twists up perceptibly inescapable, touchier information are being united into the cloud. For the protection of data insurance, fragile data generally have tube mixed before outsourcing, which influences effective data to utilize a to a great degree troublesome task. Yet standard available encryption designs empower a customer to securely look for over mixed data through watchwords and particularly recoup records of interest, these frameworks support simply amend catchphrase look. That is, there is no flexibility of minor linguistic mix-ups and association inconsistencies which, on the other hand, are average customer looking for direct and happen constantly. This basic weakness makes existing methodologies unsatisfactory in Cloud Computing as it fantastically impacts system convenience, rendering customer looking for experiences to a great degree frustrating and structure reasonability low. In this paper, all of a sudden we formalize and deal with the issue of convincing feathery catchphrase look for over mixed cloud data while keeping up watchword security. Fleecy watchword look for remarkably enhances structure comfort by reestablishing the organizing records when customers' looking information sources decisively facilitate the predefined catchphrases or the closest possible planning archives in perspective of watchword equivalence semantics, when revise coordinate crashes and burns. In our answer, we mishandle change detachment to quantify watchwords closeness and develop a moved technique on creating feathery catchphrase sets, which tremendously diminishes the limit and depiction overheads. Through intensive security examination, we exhibit that our proposed plan is secure and insurance defending, while precisely understanding the target of fleecy watchword look.

6. Cong Wang, Ning Cao, Jin Li, KuiRen, and Wenjing Lo in 2010. Secure Ranked Keyword Search over Encrypted Cloud Data. The main event when we describe and deal with the issue of reasonable yet secure situated catchphrase investigate mixed cloud data. Situated look exceptionally redesigns system comfort by reestablishing the planning archives in a situated orchestrate as for certain essentialness criteria (e.g., catchphrase repeat), in this way making one piece closer towards helpful association of security ensuring data encouraging organizations in Cloud Computing. We at first give an unmistakable yet idealize improvement of situated watchword look for under the best in class open symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To finish more valuable execution, we by then propose a definition for situated available symmetric encryption, and give a beneficial arrangement by suitably utilizing the current cryptographic primitive, organize sparing symmetric encryption (OPSE). Cautious examination exhibits that our proposed course of action acknowledges "as-strong as could reasonably be expected" security guarantee diverged from past SSE designs, while adequately understanding the target of situated watchword look for. Expansive trial comes to fruition demonstrate the capability of the proposed game plan.

7. Hongwei Li, Yi Yang, Tom H. Luan,Xiaohui Liang, Liang Zhouand Xuemin (Sherman) Shen in 2015. Empowering Fine-Grained Multi-Keyword Search Supporting Classified Sub-Dictionaries Over Encrypted Cloud Data. In this paper, we have inspected on the fine-grained multikeyword look for (FMS) issue over mixed cloud data, and proposed two FMS designs. The FMS I consolidates both the significance scores and the slant components of watchwords to enhance more correct request and better customers' seeing, independently. The FMS II finishes secure and successful chase with feasible convenience, i.e., "AND", "OR" and "NO" operations of watchwords. Also, we have proposed the overhauled plans supporting assembled sub-vocabularies (FMSCS) to upgrade efficiency. In such a framework, the individual can remotely store her data on the cloud server, specifically data outsourcing, and after that impact the cloud data to open for not anything through the cloud server. This addresses a more flexible, simplicity and stable way for open data get to because of the flexibility and high capability of cloud servers, and in this way is perfect to little endeavors. The proposed plan can reinforce convoluted method of reasoning look through the mixed "AND", "OR" and "NO" operations of watchwords. Third, we furthermore use the gathered sub-dictionaries strategy to achieve better efficiency on record building, trapdoor making and question. Eventually, we separate the security of the proposed plans similarly as mystery of records, security protection of rundown and trapdoor, and unlink limit of trapdoor.

8. Bing Wang Shucheng YuWenjing LouY. Thomas Houin 2014. Security Preserving Multi-Keyword Fuzzy Search over Encrypted Data inthe Cloud. To restrain the risk of data spillage to the cloud master associations, data proprietors pick to encode their sensitive data, e.g.,

prosperity records, cash related trades, already outsourcing to the cloud, while holding the unscrambling keys to themselves and other endorsed customers. This subsequently renders data use a testing issue. For example, remembering the ultimate objective to look through some critical reports among a mixed enlightening record set away in the cloud, one may need to download and unravel the entire instructive file. The back and forth movement feathery chase designs rely upon building a broadened list that spreads possible catchphrase wrong spelling, which provoke through and through greater record archive measure and higher interest unusualness. In this paper, we propose a novel multi-watchword cushy interest plan by abusing the territory unstable hashing system. Our proposed plot finishes cushioned organizing through algorithmic arrangement rather than developing the record report. It in like manner murders the need of a predefined word reference and effectively supports various watchword cushioned journeys without extending the document or request eccentrics. In this paper, we took care of the testing multi-watchword feathery chase issue over the mixed data. We proposed and consolidated a couple of imaginative blueprints to clarify the distinctive watchwords look for and the fleecy request issues in the meantime with high capability. Our approach of using LSH works in the Bloom channel to build up the archive record is novel and gives a successful response for the secured feathery quest for different watchwords. Additionally, the Euclidean division is grasped to get the similarity between the catchphrases and the safe internal thing count is used to discover the likeness score keeping in mind the end goal to enable outcome situating.

9. Wenhai Sun, Bing Wang, Ning Cao in 2008Protection Preserving Multi-Keyword Text Search In The Cloud Supporting Similarity-Based Ranking. We display a security sparing multi-watchword content request (MTS) plot with similarity based situating to address this issue. To help multi-watchword interest and question yield situating, we propose to make the request record in perspective of term repeat and the vector space show with cosine similarity measure to fulfill higher thing precision. To upgrade the chase capability, we propose a tree-based rundown structure and diverse adaption procedures for multi-dimensional (MD) computation with the objective that the valuable request viability is endlessly enhanced than that of direct interest. The concentrated organization of adaptable resources, all players in this rising X-as-an advantage (XaaS) illustrate, including the cloud provider, application planners, and end-customers, can get rewards. Especially, for the end-customers, they can outsource broad volumes of data and workloads to the cloud and welcome the in every practical sense unlimited figuring resources in a pay for each use way. Without a doubt, numerous associations, affiliations, and individual customers have adopte the cloud stage to energize their business operations, investigate, or consistent necessities. In this paper, as a basic undertaking to finish rational and convincing multi-watchword content interest over encoded cloud data, we make responsibilities in two imperative perspectives, supporting resemblance based situating for more correct question thing and a tree-based request count that achieves better than coordinate chase capability. For the precision point of view, we at first manhandle the outstanding comparability measure, i.e., vector space appear with cosine measure, to enough secure the exact question yield. We propose two secure rundown intends to meet distinctive insurance essentials in the two threat models. Over the long haul, the spillage of fragile repeat information can be kept up a key separation.

10. Cong Wangy, Kui Reny, Shucheng Yux, and Karthik Mahendra Raje Urs in 2013. Accomplishing Usable and Privacy-Assured Similarity Search over Outsourced Cloud Data. In this way, it is getting more pervasive than some other time in late memory for data proprietors to outsource the psyche boggling data organization structures from close-by machines to cloud for the titanic versatility and cost reserves. However, to guarantee data security and fight unconstrained gets to in cloud and past, sensitive data must be mixed by data proprietors before outsourcing. Considering the generous number of on-ask for data customers and huge measure of outsourced data records in cloud, the issue is particularly trying, as it is to an incredible degree difficult to meet in like manner the realistic requirements of execution, structure comfort, and anomalous state customer looking for experiences. We formally show the insurance sparing affirmation of the proposed part under exhaustive security treatment. To show the comprehensive proclamation of our instrument and further upgrade the application go, we moreover exhibit our new improvement ordinarily supports fleecy interest, a some time ago considered idea directing just toward bear linguistic oversights and depiction anomalies in the customer looking for input. The expansive tests on Amazon cloud organize with honest to goodness instructive gathering furthermore show the authenticity and presence of mind of the proposed framework. In this paper, roused by finishing sensible structure. Comfort and strange state customer looking for learning, we inspect the issue on secure and profitable similarity investigate outsourced cloud data. With modify evacuate as the similarity metric, our segment design at first misuse a smothering technique to create limit beneficial resemblance catchphrase set from a given report amassing. Using that watchword set as an introduce, we by then propose another picture based trie-cross looking segment, and show it viably finishes the described likeness look for with enduring request time multifaceted nature.

III. PROPOSED WORK

A. Login/New User: In this module, the login advancement itself has heaps of security. More often than not, the client account name and fitting secret key of that record are adequate to do the defense and login process, however here some more activities are given to make more

*B. Upload File:*In this module, we need to stack the information archive at that point read the information

report document and need to execute the preprocessing to that info record. With the goal that the record appended can be handled to the following stages.

C. SEARCH

1. Frequent Search: In this module, we get the non-stop words as input and calculate the count of words and find the repeated occurrence of each and every word from the non-stop words.

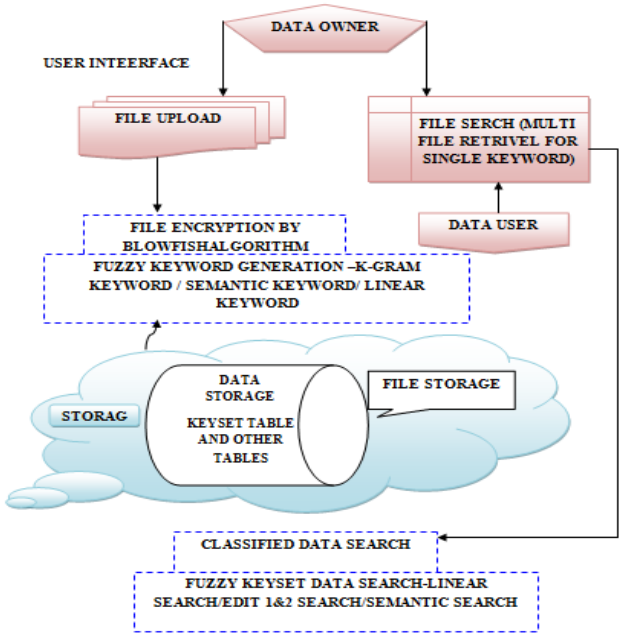

Fig 1.system architecture

2. Similarity Search: From the maximum frequents word we find the weight age of the each and every word than from the weight age value to going to calculate the similarity between the words, based on the similarity we going to group the words into clusters.

3. Linear search: In this module we are going to create search regarding the keywords, each cluster has n number of similar words as keywords this words we going to find the file for that cluster with the help of lexical analysis tool.

D. Mail alert process: The transferring and downloading procedure of the client is first get the mystery enter in the relating client email id and afterward apply the mystery key to scrambled information to send the server stockpiling and unscrambles it by utilizing his mystery key to download the comparing information record in the server stockpiling framework's the mystery key transformation utilizing the Share Key Gen (SKA, t, m)..

E. File Downloading process: Record downloading process is to get the comparing mystery key to the relating document to the client mail id and afterward decode the document information. The document downloading process decoding key to capacity servers with the end goal that capacity servers play out the unscrambling Operation. Also, the document is downloaded.

IV. ALGORITHMS

A. Blowfish

Blowfish is a symmetric square code that can be utilized as a drop-in substitution for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, fabricates it perfect for both local and exportable utilize. Blowfish was planned in 1993 by Bruce Schneider as a quick, free extraordinary to existing encryption calculations.

Quick: It scrambles information on vast 32-bit chip at a rate of 26 clock cycles for every bite.

Smaller: It can keep running in under 5K of memory.

Straightforward: It utilizes expansion, XOR, query table with 32-bit operands.

Secure: The key length is variable, it can be in the scope of 32~448 bits: default 128 bits key length.

Field	Type	Comment
filename	varchar(50) NULL	
keywrd	varchar(50) NULL	
insrt	varchar(5500) NULL	
subr	varchar(5500) NULL	
delt	varchar(5500) NULL	
insrt1	varchar(5500) NULL	
subr1	varchar(5500) NULL	
delt1	varchar(5500) NULL	
insrt2	varchar(5500) NULL	
subr2	varchar(5500) NULL	
delt2	varchar(5500) NULL	

Fig 2 Keyword table

Field	Type	Comment
usernames	varchar(50) NULL	
filenames	varchar(100) NULL	
keywords	varchar(100) NULL	
len	int(2) NULL	
status	varchar(10) NULL	

Fig 3 status table

Field	Type	Comment
username	varchar(30) NULL	
filename	varchar(30) NULL	
keywords	varchar(30) NULL	
length	varchar(5) NULL	
status	varchar(30) NULL	

Fig 4file upload

V. CONCLUSION

A secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. The cloud server traverses different paths on the index, and the data user receives different results but with the same high level of query accuracies in the meantime. The keyword-based search is such one widely used data operator in many database and information retrieval applications, and its traditional processing methods cannot be directly applied to encrypted data. Therefore, how to

process such queries over encrypted data and at the same time guarantee data privacy. Then, in order to improve the search efficiency, we design the group multi-keyword top-*k* search scheme, which divides the dictionary into multiple groups and only needs to store In the sense no need to give exact filename to download the file, if you are going to give maximum number of time repeated words, that time also original file will be downloaded in decrypted format. This helps to maintain the security of the files in the cloud.

REFERENCES

[1] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. SP 2000.Proceedings. 2000 IEEE Symposium on, 2000, pp. 44–55.

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

[3] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2016.

[4] W. M. Liu, L. Wang, P. Cheng, K. Ren, S. Zhu, and M. Debbabi, "Pptp: Privacy-preserving traffic padding in web-based applications," IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 6, Nov 2014.

[5] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1–5.

[6] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Distributed ComputingSystems (ICDCS), IEEE 30th International Conference on, 2010, pp. 253–262.

[7] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325, May- June 2016.

[8] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy preserving multi-keyword fuzzy search over encrypted data in the cloud," in INFOCOM, 2014 Proceedings IEEE, 2014, pp. 2112–2120.

[9] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proceedings of the 8th ACM SIGSAC Symposium on Information, ser. ASIA CCS '13. ACM, 2013, pp. 71–82.

[10] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in INFOCOM, 2012 Proceedings IEEE, 2012, pp. 451–459.

[11] A.Swaminathan, Y. Mao, G. M. Su, H. Gou, A. Varna, S. He, M. Wu, and D. Oard, "Confidentiality-preserving rank-ordered search," in Proc. ACM ACM Workshop Storage Security Survivability, Alexandria, VA, 2007, pp. 7–12.

[12] C. Wang, N. Cao, K. Ren, and W. J. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467–1479, Aug. 2012.

[13] D. X. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Priv., BERKELEY, CA, 2000, pp. 44–55.

[14] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. EUROCRYPT, Interlaken, SWITZERLAND, 2004, pp. 506–522.

[15] C. Wang, N. Cao, J. Li, K. Ren, and W. J. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE 30th Int. Conf. Distrib. Comput. Syst., Genova, ITALY, 2010, pp. 253–262.

[16] C. Chen, X. J. Zhu, P. S. Shen, and J. K. Hu, "A hierarchical clustering method For big data oriented ciphertext search," in Proc. IEEE INFOCOM, Workshop on Security and Privacy in Big Data, Toronto, Canada, 2014, pp. 559–564.

[17] S. C. Yu, C. Wang, K. Ren, and W. J. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM, San Diego, CA, 2010, pp. 1–9.

[18] D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M. C. Rosu, and M. Steiner, "Dynamic searchable encryption in very large databases: Data structures and implementation," in Proc. Netw. Distrib. Syst. Security Symp., vol. 14, 2014, Doi: http://dx.doi.org/ 10.14722/ndss.2014.23264

[19] S. Grzonkowski, P. M. Corcoran, and T.Coughlin, "Security analysis of authentication protocols for next-generation mobile and CE cloud services," in Proc. IEEE Int. Conf. Consumer Electron.2011, Berlin, Germany, 2011, pp. 83–87.

[20] M. Naor and K. Nissim, "Certificate revocation and certificate update," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 561–570, Apr. 2000