

A Survey on Searchable Encryption Schemes

Akash A. Khandagale¹ Nitin Gadave² Abhijit Dhok³ Suvarna Sabale⁴ Prof. Rupali Patil⁵

^{1,2,3,4,5}Department of Computer Engineering

^{1,2,3,4,5}P.G.M.C.O.E. Wagholi, Pune

Abstract— Exponential growth of web users throughout the world raises the difficulty of knowledge storage within the business. As the answer to the present cloud system plays a significant role. Because of lack of internal security at the cloud service supplier finish, cloud data storage is essentially betting on the cryptologic techniques. Though ancient searchable encoding schemes enable users to firmly search over encrypted knowledge through keywords mistreatment Boolean values. Thus there's a far urge is arises to check these systems that truly performs searching techniques and to search out their weakness. Many searching techniques square measure existed supported similarity, keyword matching, formal logic and plenty of a lot of ideas as mentioned during this paper. However most of them square measure concentrating on taking as many as a lot of documents for the given question. These techniques are literally will increase the time complexness of the searching techniques albeit they supply correct results.

Key words: Encryption, Searchable Encryption Schemes

I. INTRODUCTION

Industries were looking for some style of major answer, since utility computing terminated up changing into one thing of an enormous business for firms like IBM. Indeed, Martin Greenberger pointed out the idea that “advanced pure mathematics machines of the future” were currently being employed not solely institutionally for scientific calculation and analysis however also for business functions like accounting and inventory. Further, he anticipated his piece of labor in which computers would be universal nearly just like the major power firms running wires everywhere in due time. As the technology enhances, the question was immediately raised whether or not “Information utility” would become regulate just like the power trade or be a non-public entity in and of itself. Afterward IBM saw the potential for enormous profit to be created during this kind of business and took into thought by providing computing services to companies for high greenback. The technical limitations on bandwidth further as space were an enormous constraint on what might are developed. The paradigm for this type of data was merely not in situation to guage. However for cloud computation to require into thought, though the use of mainframe process still tested to be profitable for quite your time. Due to a revolutionary amendment within the field of industries over past decade, there has been increase in demand of outsourcing of knowledge over a good vary of network. In order to manipulate this immense quantity of knowledge in value effective manner enterprise has custom-made a current technology known as cloud computing that take away the burden of knowledge management.

During this information driven setting enterprise tend to store their information onto cloud that compromise of valuable quality of client information like emails, personal health data etc. Cloud computing is popping intent on be most essential paradigm within the development of

data technology which provide versatile access , ubiquitous, on demand access and cost saving . Despite its technical advantage in business, enterprise should always keep concern of its privacy from the prying eyes over a network. Privacy protective is one amongst the foremost hurdles in cloud for user, particularly once the user information that reside in native storage is outsourced and computed onto cloud. The sensitive information that a cloud service supplier is holding can be secure by firewalls, intrusion detection system additionally CSP has full management over the infrastructure of cloud as well as lower level of system stack and system hardware. Though mitigate concern area unit taken still privacy breaches is probably going to occur within the paradigm. In few cases the service supplier isn't totally sure, however still we'd like the service. Therefore, some methodology ought to be authorized to protect the user information and user queries from unauthorized person within the cloud setting.



Cloud Computing

Having secure access to all your applications and data from any network device

Fig. 1: Working of Cloud Computing

Thus, before causing information onto the cloud, information should be encrypted to shield from information privacy and unsought access. However several user believe that encoding of information before outsourcing offer a robust guarantee that the information privacy would be maintain against the cloud service providers. as an example, the user might cipher a email body by employing a public key before causing it to the service provider then send the information to the service supplier. Since, public secret is illustrious solely to the user the service provider couldn't breach the privacy of email. Though encryption provides privacy, it makes information utilization a challenging task specified it complicates the computation on the information like the basic search operation being carried out on cloud. While not keyword search operate the cloud can become a far off storage that provides restricted value to all or any the enterprises that store its information on the cloud. Still, cloud wouldn't offer an economical search on the encrypted information to approve the advantages of a full-fledged cloud computing atmosphere.

II. RELATED WORK

Encryption is associated as the best route to stay the privacy of the info. On another facet search operation on such information is very difficult task. Variety of search techniques had been enforced to perform this one. In spite of this searching information on this cloud is facing some severe problems. Currently now a day cloud computing is on look. Normally the scale of the standalone system isn't enough to store massive information, this downside of storage is simply overcome by the cloud computing. A survey was conducted by David Simms and he found that just about ninety fifth of peoples are believe cloud for their storage. The largest advantage offers by the clouds area unit information outsourcing. Typically third party vendor area unit there to produce the cloud services that reduce the burden of maintaining cloud because it maintains by that third party solely. With this nice advantage, if utilization of such information isn't correct then there'll be no use of those blessings. As security is one amongst the most issues of the cloud data, authority a cloud community offers some options to protect information from trapdoors. Thus the most challenge in cloud computing is effective looking out. Previously looking out is appropriate for under unencrypted information which doesn't offers security over cloud thence secret writing of data came into existence. And to go looking over such encrypted information is difficult task. This paper focuses on the same down side, it provides completely different keyword search methods for encrypted information over cloud. Traditionally it's seen that plaintext technique cannot be applied on to search the need information. Multi -key word hierarchal search has historically been provided by Information Retrieval system (IRS) for information user. To overcome the problem of looking out on encrypted information a algorithm has been planned by [1], that represented a problem of multi-keyword search over encrypted information victimisation .Latent-linguistics -Analysis, that not solely come the file including the terms latent semantically related to keyword question however additionally come the precise matching file. It uses the vector consisting of TF values that analyse the latent linguistics association between terms and documents by LSA .Security and privacy is enforce by employing a cacophonous k-NN technique to write the index and therefore the queried vector, so that we will get the correct result. [2] Address, content-based transmission retrieval over encrypted databases that change consumer retrieval directly within the encrypted domain. so as to secure index theme like mini-Hash sketches and secure inverted index it uses collectively exploiting technique like cryptography, image process, and information retrieval. the primary schema exploits randomized hash functions and therefore the second schema makes use of inverted indexes of visual words. This model is further increased to beat mini- Hash theme that require longer sketches to attain higher performance in order to attain performance kind of like that of the inverted index theme. To retrieve a document containing solely a word [3] describe, a crypto-logical model that focuses on downside of searching AN encrypted information and supply a secure cryptosystem. this system target hidden question in order that the untrusted server cannot seek for a word while not the user's authorization and it additionally support question isolation means that, the server learns nothing quite the

result. It provides An approach to go looking over remotely situated information .In this method document retrieval is finished in 2 phases.

Here independent public key secret writing technique may be opt for, also it's appropriate for various file formats that add a lot of weightage to the current technique. However it needs extra storage overhead and cannot guarantees the safety of the info. With this nice advantage, if utilization of such information isn't correct then there'll be no use of those blessings. As security is one amongst the most issues of the cloud data, authority a cloud community offers some options to protect information from trapdoors. Thus the most challenge in cloud computing is effective looking out. Previously looking out is appropriate for under unencrypted information which doesn't offers security over cloud thence secret writing of data came into existence. And to go looking over such encrypted information is difficult task. This paper focuses on the same downside, it provides completely different keyword search methods for encrypted information over cloud. Traditionally it's seen that plaintext technique cannot be applied on to search the need information. Multi -key word hierarchal search has historically been provided by Information Retrieval system (IRS) for information user. To overcome the problem of looking out on encrypted information a algorithm has been planned by [1], that represented a problem of multi-keyword search over encrypted information victimization. Latent- linguistics -Analysis, that not solely come the including the terms latent semantically related to keyword question however additionally come the precise matching file. It uses the vector consisting of TF values that analyse the latent linguistics association between terms and documents by LSA .Security and privacy is enforce by employing a cacophonous k-NN technique to write the index and therefore the queried vector, so that we will get the correct result. [2] Address, content-based transmission retrieval over encrypted databases that change consumer retrieval directly within the encrypted domain. so as to secure index theme like mini-Hash sketches and secure inverted index it uses collectively exploiting technique like cryptography, image process, and information retrieval. the primary schema exploits randomized hash functions and therefore the second schema makes use of inverted indexes of visual words. This model is further increased to beat mini- Hash theme that require longer sketches to attain higher performance in order to attain performance kind of like that of the inverted index theme.

To retrieve a document containing solely a word [3] describe, a crypto-logical model that focuses on downside of searching AN encrypted information and supply a secure crypto system. this system target hidden question in order that the untrusted server cannot seek for a word while not the user's authorization and it additionally support question isolation means that, the server learns nothing quite the result. It provides AN approach to go looking over remotely situated information .In this method document retrieval is finished in 2 phases. Here independent public key secret writing technique may be opt for, also it's appropriate for various file formats that add a lot of weightage to the current technique. However it needs extra storage overhead and cannot guarantees the safety of the info. With this nice advantage, if utilization of such

information isn't correct then there'll be no use of those blessings. As security is one amongst the most issues of the cloud data, authority a cloud community offers some options to protect information from trapdoors. Thus the most challenge in cloud computing is effective looking out. Previously looking out is appropriate for under unencrypted information which doesn't offers security over cloud thence secret writing of data came into existence. And to go looking over such encrypted information is difficult task. This paper focuses on the same downside, it provides completely different keyword search methods for encrypted information over cloud. Traditionally it's seen that plaintext technique cannot be applied on to search the need information. Multi -key word hierarchal search has historically been provided by Information Retrieval system (IRS) for information user. To overcome the problem of looking out on encrypted information a algorithm has been planned by [1], that represented a problem of multi-keyword search over encrypted information victimisation Latent-linguistics -Analysis, that not solely come the file including the terms latent semantically related to keyword question however additionally come the precise matching file. It uses the vector consisting of TF values that analyse the latent linguistics association between terms and documents by LSA .Security and privacy is enforce by employing a cacophonous k-NN technique to write the index and therefore the queried vector, so that we will get the correct result. [2] Address, content-based transmission retrieval over encrypted databases that change consumer retrieval directly within the encrypted domain. so as to secure index theme like mini-Hash sketches and secure inverted index it uses collectively exploiting technique like cryptography, image process, and information retrieval. the primary schema exploits randomized hash functions and therefore the second schema makes use of inverted indexes of visual words. This model is further increased to beat mini- Hash theme that require longer sketches to attain higher performance in order to attain performance kind of like that of the inverted index theme. To retrieve a document containing solely a word [3] describe, a crypto-logical model that focuses on downside of searching AN encrypted information and supply a secure cryptosystem. this system target hidden question in order that the untrusted server cannot seek for a word while not the user's authorization and it additionally support question isolation means that, the server learns nothing quite the result. It provides AN approach to go looking over remotely situated information .In this method document retrieval is finished in 2 phases. Here independent public key secret writing technique may be opt for, also it's appropriate for various file formats that add a lot of weightage to the current technique. However it needs extra storage overhead and can not guarantees the safety of the info. With this nice advantage, if utilization of such information isn't correct then there'll be no use of those blessings. As security is one amongst the most issues of the cloud data, authority a cloud community offers some options to protect information from trapdoors. Thus the most challenge in cloud computing is effective looking out. Previously looking out is appropriate for under unencrypted information which doesn't offers security over cloud thence secret writing of data came into existence. And to go looking over such encrypted information is difficult task. This paper focuses on the same

downside, it provides completely different keyword search methods for encrypted information over cloud. Traditionally it's seen that plaintext technique cannot be applied on to search the need information. Multi -key word hierarchal search has historically been provided by Information Retrieval system (IRS) for information user.

To overcome the problem of looking out on encrypted information an algorithm has been planned by [1], that represented a problem of multi-keyword search over encrypted information victimization. Latent- linguistics - Analysis, that not solely come the file including the terms latent semantically related to keyword question however additionally come the precise matching file. It uses the vector consisting of TF values that analyse the latent linguistics association between terms and documents by LSA .Security and privacy is enforce by employing a cacophonous k-NN technique to write the index and therefore the queried vector, so that we will get the correct result. [2] Address, content-based transmission retrieval over encrypted databases that change consumer retrieval directly within the encrypted domain. so as to secure index theme like mini-Hash sketches and secure inverted index it uses collectively exploiting technique like cryptography, image process, and information retrieval. The primary schema exploits randomized hash functions and therefore the second schema makes use of inverted indexes of visual words. This model is further increased to beat mini- Hash theme that require longer sketches to attain higher performance in order to attain performance kind of like that of the inverted index theme. To retrieve a document containing solely a word [3] describe, a crypto-logical model that focuses on downside of searching AN encrypted information and supply a secure crypto system. this system target hidden question in order that the untrusted server cannot seek for a word while not the user's authorization and it additionally support question isolation means that, the server learns nothing quite the result. It provides AN approach to go looking over remotely situated information .In this method document retrieval is finished in 2 phases. Here independent public key secret writing technique may be opt for, With this nice advantage, if utilization of such information isn't correct then there'll be no use of those blessings. As security is one amongst the most issues of the cloud data, authority a cloud community offers some options to protect information from trapdoors. Thus the most challenge in cloud computing is effective looking out. Previously looking out is appropriate for under unencrypted information which doesn't offers security over cloud thence secret writing of data came into existence. And to go looking over such encrypted information is difficult task. This paper focuses on the same downside, it provides completely different keyword search methods for encrypted information over cloud. Traditionally it's seen that plaintext technique cannot be applied on to search the need information. Multi - key word hierarchal search has historically been provided by Information Retrieval system (IRS) for information user. To overcome the problem of looking out on encrypted information a algorithm has been planned by [1], that represented a problem of multi-keyword search over encrypted information victimization. Latent-linguistics -Analysis, that not solely come the file including the terms latent semantically related to keyword question however additionally come the precise matching file. It uses

the vector consisting of TF values that analyse the latent linguistics association between terms and documents by LSA. Security and privacy is enforced by employing a cacophonous k-NN technique to write the index and therefore the queried vector, so that we will get the correct result. [2] Address, content-based transmission retrieval over encrypted databases that change consumer retrieval directly within the encrypted domain. So as to secure index theme like mini-Hash sketches and secure inverted index it uses collectively exploiting technique like cryptography, image process, and information retrieval. The primary schema exploits randomized hash functions and therefore the second schema makes use of inverted indexes of visual words. This model is further increased to beat mini-Hash theme that require longer sketches to attain higher performance in order to attain performance kind of like that of the inverted index theme. To retrieve a document containing solely a word [3] describe, a crypto-logical model that focuses on downside of searching AN encrypted information and supply a secure crypto system. this system target hidden question in order that the untrusted server cannot seek for a word while not the user's authorization and it additionally support question isolation means that, the server learns nothing quite the result. It provides AN approach to go looking over remotely situated information. In this method document retrieval is finished in 2 phases. Here independent public key secret writing technique may be opt for, also it's appropriate for various file formats that add a lot of weightage to the current technique. However it needs extra storage overhead and cannot guarantees the safety of the info. Also it's appropriate for various file formats that add a lot of weightage to the current technique. However it needs extra storage overhead and cannot guarantees the safety of the info. Quin Liuy, Guojun Wangyz, and Jie Wuz [4] say if CSP is employed on looking then system can face the matter of security. One resolution on this is often to use cryptologic approach which will manage the approved users that have access to such information. The authors try and preserve the privacy of the info, keyword and also the linguistics of the info. All technique relies on the general public key secret writing. It makes use of CSP for the decoding purpose. Unlike Associate in Nursing other ways it mentioned an SPKS approach wherever cloud service supplier is truly gets concerned. The role of the cloud service supplier is to try and do decipher text of cipher text. By doing this process value of user for the cryptography of encrypted knowledge are often scale back considerably. Here decryption is completed by the cloud service supplier however he really not aware of the keyword and knowledge within which keyword is to be searched. To try and do experimental analysis system performance is compared with the Boneh et al system. It makes use of CSP for the cryptography purpose. Ming li [5] states the approved non-public keyword search techniques that gives the privacy of the information, question conjointly a multidimensional keyword looking out operations. Advanced to this he planned APKS+. The primary methodology enhances the efficiency of looking out algorithms and therefore the second methodology preserves the privacy of the question. Here the matter of authorised looking out of keyword is mentioned. During this paper two approaches scientific discipline primitive and hierarchal Predicate cryptography area unit planned. This technique

makes use of personal health records for the aim of testing the system. The higher than techniques can get fails if entity synonyms or morphological variants area unit used. On distinction to the current Cong [6] states search operations on encrypted information can increase the price of processing and traffic of network. Cong Wang planned a new looking theory that reduces the process overhead that usually obstacles the search system. Author uses build index on and also the keyword frequency primarily based relevance score. It implements a secure stratified primarily based keyword search methodology. During this methodology order protective mapping theme is employed wherever little encrypted files square measure processed 1st then giant encrypted files square measure processed. Authors gift a theory for retrieving documents that makes use of stratified Searchable bi-radial secret writing, Order protective bi-radial secret writing and one several Order protective Mapping. This methodology is employed to realize a great accuracy and security. Additionally it avoids unwanted retrieval and traffic drawback. However system fails if multiple keywords square measure fed as input, with such input looking speed also will increase. The on top of explicit Ways square measure supported precise query matching however it didn't implement the similarity matching. Boneh et al. [7] planned a awfully 1st PKC primarily based search theme once he galvanized from the identity primarily based encryption. This theme is an intition well matched for single query only. By victimisation this theme anyone with public will write to cloud however the user having a non-public key will solely allow playing looking operations on cloud. By taking base of this system, variety of methodologies have been enforced to filter the looking techniques. One of the good author Li [8] planned another predictive secret writing technique that relies on the hierarchical secret writing. this system build licensed keyword search technique over cloud. Like another techniques this system additionally provides search access to the authorized users and non-authorized users won't get access to go looking. In spite of effectiveness of those schemes it has biggest downside that it's computationally expensive. In [9] authors attempt to solve the matter of looking out over encrypted knowledge in cloud. It makes use of confidentiality preserving ordering technique. This methodology forms the framework by mistreatment secure index, encrypted domain search and hierarchical retrieval for the extraction of information from the cloud. betting on encrypted queries it ranks the documents and document having most rank are going to be pushed up mistreatment hierarchical methodology. The given methodology is well matched for large documents and additionally It provides higher accuracy and security. Except for this methodology machine price is high and protective communication link is bit tough task. Dan Boneh et.al. [10] Presents associate attribute primarily based encryption approach with prediction secret writing theme. The drawbacks of 1 technique ar simply overcome by another theme. Since it makes use of 2 totally different schemes it's extremely secure and quicker. Since on cloud the data is found kind remote locations, thus it's challenging task to access and retrieve knowledge kind such remotely situated info. Here Smith generate a 1 key for the e-mail entranceway and by mistreatment this key email gateway get access to examine

“urgent” keyword in email without reading the whole email. By doing that the desirable work of each parties will be done and therefore the privacy of the system additionally won't get compromised. Here identity based secret writing is employed for the aim of the secret writing. The disadvantages of the on top of systems are: one refreshing keywords, 2.secure channel removal, 3.multiple keyword processing. [11] Makes use of PIR queries for looking out over cloud. This methodology uses bloom filter provides storage space which might be helpful to store some further info. It hides the identity of the communication additionally keeps the semantic of the encrypted knowledge. However it'll not preserve the privacy and correctness of the info. Mehmet Kuzu [12] introduces a technique of section sensitive hashing that may be a high dimensional area searching technique .which uses a hashing technique to create door for looking out encrypted documents within the cloud. Because the hashing technique is a way it can't reverse engineer to recheck the outcomes and additionally this method takes short while to go looking the document because of granular hashing method. Ming Li et al. [13] provides a completely unique approach for privacy conserving looking out paradigm.

The looking out approaches are accustomed search keyword over cloud knowledge that are outsourced from the third parties. Here 2 forms of Searching approaches are used: one. Ranked over keyword search and a pair of. Search over structured knowledge. The reason behind mistreatment of those techniques is their quality within the field of data retrieval in plain domain. In above technique confidentiality is obtained go did not offer variability once looking out on encrypted knowledge is finished. Jianfeng Wang et al. [14] Presents a very important approach that not solely warranty the confidentiality and security however additionally the verifiability of the looking out methodology. Verifiability refers to cross check condition that typically done to be safe on our facet. An emblem tree primarily based looking out is done encrypted knowledge to attain the goal. The rationale to use mathematical logic for the planned approach is same as same above. Here for the terribly 1st time mathematical logic primarily based keyword search technique for encrypted knowledge is planned great security of knowledge is achieved whereas protective theprivacy of the info. Associate in Nursing experiment shows that for every query system can offer the constant price of complexness.

Also the process price is reduced from the $O(L)$ to $O(1)$ wherever L could be a length of question. Author makes use of Linux machine with Pentium twin core processor for the purpose of experiments.Wenhai Sun et al. [15] elaborates another similarity primarily based ranking approach for the aforesaid purpose. To get finished the task frequency of every word is use out. And earlier a vector area model with circular function similarity is used to extend the potency of the looking formula. Vector area model is employed to support conjunctive and disjunctive looking conjointly. A tree primarily based index looking with flat formula is employed. the explanation behind using this is often to hurry up the method as this speed is one amongst the main drawbacks in linear search. Any to extend the privacy of the looking algorithms 2 a lot of indexes known as cipher text model and background model is employed. So

finally author concludes that potency of looking and preciseness of looking is well balanced by the approach.

Suppose SAM desires to send email to the Smith that is encrypted by the general public key of Smith. This email is distributed through the e-mail entryway. Email entryway desires to ascertain whether email contains “urgent” keyword or not. If it contains “urgent” keyword then 1st priority is given to it message however at a similar time Smith don't need to decipher complete message by the e-mail entryway. While looking question on given domain the character of question plays a very important role. The a lot of correct the query the a lot of precise are going to be the output.

III. CONCLUSION

The higher than studied systems square measure been projected to conduct the search over the encrypted knowledge that square measure been stored on the cloud aspect. And in majority of the systems the accumulated drawback with them is, they're taking a lot of time to look the information. Authors like Jianfeng Wang et al. depicts methodology/a way/a technique} of looking knowledge exploitation tree primarily based method. with mathematical logic wherever system is stress to scale back the cost. Boneh et al. shows methodology of key primarily based looking technique. Whereas Y.-C. Chang, uses PIR question with bloom filters to look over the encrypted knowledge .So of these methods square measure ne'er talking concerning reducing the time complexity of the system. a awfully few finger enumeration systems square measure been projected to decrease the time of looking however they're additionally not with success enforced this on large amount of knowledge.

So a substantial analysis is needed to attenuate the searching time over the encrypted knowledge in cloud.

REFERENCES

- [1] Li Chen, Xingming Sun,Zhijia Xia ,Qi Liu,” An Efficient and Privacy-Preserving Semantic Multi-Keyword Ranked Search over Encrypted Cloud Data”in International Journal of Security and Its Application in 2014 .
- [2] Wenjun Lu, Ashwin Swaminathan, Avinash L. Varna, and Min Wu, “Enabling search over encrypted multimedia databases,” in proc. of SPIE Media Forensicsand Security,09,2009.
- [3] D. X. Song, D. Wagner and A.Perrig,” Practical Techniques for Searches on Encrypted Data”. Proceedings of the 2000 IEEE Symposium on Security and Privacy, pp. 44-55.
- [4] Qin Liuy, Guojun Wangyz, and Jie Wuz,”Secure and privacy preserving keyword searching for cloud storage services”, ELSEVIER Journal of Network and computer Application, March 2011
- [5] Ming Li et al.,” Authorized Private Keyword Search over Encrypted Data in Cloud Computing, IEEE proc. international conference on distributed computing systems, June 2011, pages 383-392
- [6] Cong Wang et al., ”Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud

- Data”, IEEE Transactions on parallel and distributed systems, vol. 23, no. 8, August 2012
- [7] Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Advances in CryptologyEurocrypt 2004, pp. 506–522. Springer (2004)
- [8] Li, M., Yu, S., Cao, N., Lou, W.: Authorized private keyword search over encrypted data in cloud computing. In: Distributed Computing Systems (ICDCS), 2011 31st International Conference on, pp. 383–392. IEEE (2011)
- [9] Swaminathan A, Mao Y, Su G-M, Gou H, Varna AL, He S, M. Wu, Oard D “Confidentiality Preserving Rank-Order search” Storage security and survivability 2007-Conference Papers (Proceedings of the 2007 ACM workshop on Storage security and survivability) pp.7-12.
- [10] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano “Public Key Encryption with Keyword Search” Springer Berlin Heidelberg; EUROCRYP’04, Volume: 3027 of LNCS- 2004 pp.506-522
- [11] Y.-C. Chang, M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data” conference 2005.
- [12] Mehmet Kuzu, Mohammad Saiful Islam, Murat Kantarcioglu “Efficient Similarity Search over Encrypted Data “, IEEE trasaction , 2012.
- [13] Ming Li et al., ”Toward Privacy-Assured and Searchable Cloud Data Storage Services”, IEEE Transactions on Network, volume 27, Issue 4, July/August 2013
- [14] Jianfeng Wang et al., “Efficient Verifiable Fuzzy Keyword Search over Encrypted Data in Cloud Computing”, Journal of Computer Science and Information system, volume 10, Issue 2, April 2013
- [15] Wenhai Sun et al., "Privacy-Preserving Multi- keyword Text Search in the Cloud Supporting Similarity-based Ranking", the 8th ACM Symposium on Information, Computer and Communications Security , Hangzhou, China, May 2013. Archana D. Narudkar et al, / (IJSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1007-1010 www.ijcsit.com 1010