N-Gram Fuzzy Keyword Search on Encrypted User Data in Cloud Using Jaccard Calculation

Sangeeta Wankhade
Designation: Lecturer
Dept. Information Technology
Vidyalankar Polytechnic, Mumbai, India
sangeeta.wankhade@vpt.edu.in

Dr.Prashant.P.Nitnaware
Designation: Professor
Dept. Computer Engineering
PCE, Mumbai ,India
pnitnaware@mes.ac.in

Abstract: *Now-a-days users mostly store their personal data and professional data on the cloud. As a result, there is massive increase in the storage and computing requirements of users. Every time, the data is getting transferred to the remote server in larger chunks, without analyzing whether the server on which the data is outsourced, is a trusted server or not. But the fact is, after outsourcing the data, users are at great security risk factor that tends to lose the local possession of their large size of data. So, to maintain the privacy of personal data/documents stored in cloud environment, it should first get encrypted before outsourcing to the cloud server. After the data is placed on the cloud, retrieving the same data becomes quiet a tedious job. Thus, to retrieve the data several approaches are available in which keyword enabled search of the encrypted data is one of the outstanding techniques. Most of these approaches are only limited to handle a single keyword search with its own limitations. To enhance the searching method in terms of efficiency and speed, a fuzzy multi-key word search technique can be used to retrieve a corresponding document from cloud. The scheme of fuzzy keyword search remarkably improves the system efficiency and security over the cloud environment. The proposed scheme is convenient , manageable, and even requires less resource. The outcomes of this scheme are valid enough to get the accurate files or the closet possible match files searched by the user. Thus, we have proposed a secure search scheme supporting N-Gram fuzzy multi-keyword search over encrypted cloud data.*

Keywords- N-Grams, Cloud Computing, Encryption, Fuzzy Keywords, Security.

I. INTRODUCTION

Cloud Computing is an increasing mature model of enterprise IT infrastructure that provides high demand on quality applications and services from a shared pool of configuration computing resources. To avoid the costs of building and maintaining a private storage infrastructure the cloud customers, individuals, or enterprises can outsource their local complex data system into the cloud. The company or organization's private and sensitive data like personal files, company records data, emails, etc which is to be shared among the selected different company employees is stored and in the centralized cloud server but with an insecure feeling that anyone can hack the data that may be very risky for the company.

Also, the data owners and cloud server should not be in the same trusted domain who put the outsourced unencrypted data, if any, at risk; the cloud server may leak data information to unauthorized entities or even be hacked[1][22]. Cloud enables large group of remote servers to be in a network to allow the centralized data repository, and access to the computer services or resources whenever required. Many users are inspired to outsource their confidential data on to the cloud. As the documents get transferred to the cloud, users do not have physical possession of that data. To make sure that the data at cloud side is safer, it must adapt to the privacy preserving storage methodology, as the cloud server is not a trusted server. To protect data confidentiality and unauthorized access to the cloud data, owners are motivated to encrypt their data before it is being outsourced to cloud[21][22].

To overcome this problem, the data stored in cloud storage database needs to be encrypted prior sending to cloud servers for storage. The number of cloud service client/users are increasing day by day because of increasing importance of storing the data effectively and computing models which are accessible within the cloud.

Subsequently, huge amount of data is being added into the cloud servers. Therefore, in such a scenario, the searching and retrieving operation on the file becomes very tedious because the data is in encrypted form and compel the user to search the data which is in encrypted form only. Hence, the data retrieval process becomes the cumbersome problem and a difficult job. It leads to unreliable way to access files by retrieving files excluding the relevance score thereby increasing the wastage of computation cost [23]. Nowadays, the efficient keyword searching technique acquires a paramount importance . The conventional searching methodology is not so fruitful as the user keeps the data in encrypted format at cloud side. This can be achieved by performing multi-keyword query to get the top relevant data of user interest which lead to effective searching technique on the encrypted cloud data [21][23].

1.1 MOTIVATION

Due to substantial increase in the use of cloud computing, more and more data has been uploaded by users on cloud server every day. So, it is necessary to find a solution for simple, easy, more secure, and safe method for handling the sensitive data . Hence , the solution for such problem is to use some security providing algorithms like AES 256 encryption/decryption and algorithm for checking the similarity between the data. Therefore, in this approach rather than searching the keyword directly it has been encrypted and then searched i.e., over the encrypted data which provides more security as compared to the traditional searching method. In this method, AES encryption algorithm and Base64 for encryption and Jaccard coefficient to find the similarity coefficient between the keywords is used. When the user enters the keyword, it gets converted into the encrypted keywords and then searched, and user can get the required data by the use of fuzzy keyword search methodology over encrypted cloud computing which simultaneously take care of the safety and secrecy of user's data files. The N-

Gram fuzzy keyword search greatly increases the efficiency and safety over cloud environment. This is a convenient, easy and comfortable to manage and need less resource and the results are precise enough to get exact or closet possible files searched by the user. In this approach, Jaccard coefficient is being used to calculate similarity and to determine the continuity between the entered elements of data, through which great results can be obtained. To generate different set of n-grams of varying length the N-gram algorithm is used to which is then encrypted and is being stored over cloud database.

II. LITERATURE SURVEY

Even though there are various systems existing, this literature survey mainly concentrates on the single keyword-based encryption and multi-keyword-based encryption and included other searching techniques due to it known advantages.

1. Single Keyword Search:

Deepali D. Rane et.al,[1] proposes how to implement the encryption and decryption algorithm, it uses constructing the secure index which is advantageous in terms of giving desirable performance. After index is constructed, it will get compressed and it will be get stored in the format of .cfs file. When single-keyword query is fired, user will receive all relevant documents that contains that specific keyword. Some advantages of this scheme is in protecting the data privacy by the use of encrypting documents before outsourcing, and by using rank based retrieval method of the documents, and will be able to easily access the data which is encrypted by multi keyword rank search with the help of keyword index. This scheme has some disadvantages like single-keyword search without ranking, Boolean keyword searching without ranking, single-keyword search with ranking, gives rarely sorting of the results i.e., no index is created without ranking, and useful for only single user search.

C. Wang et al,[2] has proposes a secure ranked keyword search methodology that make use of the keyword frequency to rank the results of the techniques. The main disadvantages of using single keyword search systems with or without ranking most likely will not give the relevant and desired data and it the privacy is also compromised.

Y.-C. Chang et al,[3] proposed the technique of similar type of indexes , which builds a single encrypted hash table index for the entire collection of files.

D. Song, D. Wagner et al, [4] proposes the technique of searchable encryption, in which every word in the desired document was encrypted independently under the construction of two-layered encryption method.

2. Multi-Keyword Search:

Zhihua Xia et.al,[5] has proposed a efficient, secure and dynamic search technique, which not only supports the exact multikeyword ranked search but also supports the dynamic insertion deletion and of the documents. A unique keyword balanced binary tree has been constructed as the index and proposed a "Greedy Depth-first Search" algorithm. So, this method obtains a better efficiency than linear search. To further reduce the time cost an additional parallel search process can be carried. The secure KNN algorithm is used for security of the scheme which is protected against the two threat models. The merits of the proposed system are listed as the searchable encryption schemes enables the client to store the encrypted data to the cloud and over cipher text domain keyword search query is executed and it supports multi-keyword ranked search and dynamic operation on the document collection which is secured by tree-based search scheme over the encrypted cloud data. The major drawback is without authorization the cloud service providers (CSPs) that holds the user data can easily access the user's sensitive information. This is a general approach to protect the confidentiality of data and to encrypt the data before outsourcing. This scheme however causes a huge cost in terms of data usability.

- **Bing Wang et.al,[6]** proposes a unique construction for a searchable public key encryption scheme based on inverted index technique. This scheme is specifically designed to overcomes the limitation of one-time-only search as mentioned in the earlier schemes. The demerits of the proposed system it compromises the keyword privacy once a keyword is searched. Thus, once it has been searched the index must be rebuilt for the keyword. The solution is impractical due to the high overhead which the scheme has suffered. The other flaw is that the conjunctive multi-keyword search is not supported by this scheme which is the most common form of queries. The merits are analyzing the problem of building a searchable encryption scheme based on the inverted index, attains secure and private matching between the secure index and the query trapdoor. So, a unique/novel trapdoor generation algorithm is implemented so that the related query to inverted lists are combined secretly together without letting know the cloud server which inverted lists are retrieved.

Yanzhi Ren et.al,[7] proposes a approach which supports light-weight search efficient multi-keyword ranked search in cloud computing environment. The scheme utilizes the polynomial function to lock up the encrypted keyword and search patterns for efficient multi-keyword ranked search. The basic scheme and the proposed scheme i.e a privacy-preserving which employs the security of inner product method for protecting the privacy of the searched multi-keywords is improved. It gives the advantage of guaranteed privacy of the proposed scheme and conduct extensive experiments based on the dataset of the real-world . The drawback is there is the chance of leakage of data in cloud.

Hongwei Li et.al,[8] ,multi-keyword ranked search scheme over encrypted mobile cloud data is proposed to allow efficient, accurate, and secure search. The proposed scheme successfully achieved the confidentiality of documents and index, trapdoor privacy, and covers the access pattern of the search user. The advantage of this scheme is active construction an efficient index so that it will improve the search methodology efficiently . It also achieved the enhanced efficiency in terms of functionality and search efficiency compared with existing proposals.

Mikhail Strizhov et.al,[9] proposes a technique called as a searchable encryption scheme that enables the secure searching experience over encrypted data stored on remote servers. The multi-keyword ranked search over encrypted cloud data problem is defined and solved by this scheme. It presents a well-planned similarity searchable encryption scheme that supports multi-keyword semantics. The solution to this is based on two main parameters: Term Frequency Inverse Document Frequency (TF-IDF) measurement and ring LWE-based

variant of homomorphic cryptosystem. The scheme is advantageous in terms as it returns the matching data items in a ranked ordered manner. The drawback is it supports only single keyword search.

3) Other Searching Techniques:

E.-J. Goh et al, [10] proposes a method that make use of Bloom filters to construct the indexes for the data files. For each file the Bloom filter containing trapdoors of all different words are built up and kept on the server. To search a particular word, the user needs to generate the search request by evaluating the trapdoor of the word and then sends it to the server. After receiving the request, the server performs the tests to check if any Bloom filter matches with the trapdoor of the query word and if true, the corresponding file identifiers is returned.

Jun Zhou et.al,[11] has proposed a more effective and efficient technique for verifiable outsourced computation of encrypted data EVOC. The one-way trapdoor function is implemented by just combining both addition and multiplication operations with Yao's Garbled Circuit to devise the privacy-preserving data aggregation. It demonstrates the security of the efficient privacy-preserving data aggregation proposed scheme.

Fanyu Bu et.al,[12] proposes a scheme based on BGV encryption scheme on cloud for demonstrating the privacy preserving backpropagation algorithm. The feature that the proposed algorithm includes is to apply the BGV encryption scheme to the back-propagation algorithm to prevent the disclosing of private data with cloud computing. The advantages of the scheme are :By offloading the expensive operations on the cloud it improves the efficiency of back-propagation learning. The private data is also prevented by the disclosure of using full homomorphic encryption scheme to encrypt the source data. The drawback includes during the process of the computation on the cloud the sensitive data is easily disclosed

Joseph K et.al,[13] proposes an infrastructure for sharing and searching for real-time video data securely. By deploying 5G technology and a cloud computing platform it becomes useful for mobile users. Even if the cloud server is hacked the scheme guaranteed security because the data confidentiality is now preserved by cryptographic encryption algorithms. The advantage is even if the cloud server is hacked it guarantees the security of infrastructure. The downside is that some of the existing platforms cannot simultaneously achieve secure fine-grained sharing and secure searching by sharing real time video.

Zhangjie Fu et.al,[14] proposed the scheme based on semantic search scheme that provides an efficient verifiable keyword. The proposed scheme is more practical and flexible, better suits user's different search intentions as compared to the most of the existing searchable encryption schemes. Furthermore, the proposed scheme protects privacy of data and in the presence of the semi honest server in the cloud computing environment it supports the verifiable search ability, The pros of the scheme are: the flexibility is improved and it support the verification of search results by data privacy preserving. The cons is due to the huge bandwidth and computation burden the solution of downloading the whole encrypted data first and then decrypting it locally is obviously unrealistic and insignificant.

Jin Li et al,[15] proposes a new search methodology that uses the fuzzy keyword search. It targets on enabling effective and efficient privacy preserving fuzzy keyword search in Cloud Computing. While maintaining keyword privacy, it formalizes the problem of effective fuzzy keyword search over encrypted cloud data.

D. Boneh, G. D. Crescenzo et.al,[16] proposes a searchable encryption technique , in which anyone can write to the data stored in server who has the public key but with one restriction that only registered and authorized users can search with the help of private key. The public key are very expensive in terms of computation that is the major drawbacks of using public key. In addition to that, the privacy of keyword may possibly not be protected in the public key setting, as because the server possesses the ability to perform encryption on any keyword with the public key Thus , the demerit is it used to acquire the trapdoor to get the cipher text.

Utkarsh Joshi1 , Neeraj Vishwakarma , A.Murugan, [17] proposed a Fuzzy Keyword Search over Encrypted Data scheme which focuses on using Advanced Encryption Standard (AES) for storing data securely and to perform fuzzy keyword searching on the encrypted data for retrieving the information .The traditional searchable encryption schemes provide a range of techniques to search on encrypted data, but it only reinforces on the exact keyword search. Exact keyword search is not acceptable for cloud storage systems, because it doesn't allow users to make any kind of spelling errors or format inconsistencies, which leads to greatly reducing the system usability. Perhaps, the "Wildcard-based Fuzzy Set Construction" is the most feasible scheme published so far which supports fuzzy keyword search. This technique returns the matching files when users search query input exactly match the predefined set of keywords or when exact match fails it then returns the closest possible matching files based on similarity keyword semantics.

Dr.Narendra Shekokar , Kunjita Sampat, Chandni Chandawalli ,Janvhi Shah,[18] proposes the implementation of fuzzy keyword search over encrypted data in cloud computing. This method gives the execution of the protection of important exclusive information by encrypting the outsourced data into the cloud .The current techniques allows the user to search over encrypted data with only the exact keywords. The scheme does not support any kind of typos mistakes and format variability which are normal user behavior . And ultimately results in making the user searching experience very frustrating and it makes the effective data storage process and utilization a very challenging task and thus makes the system inefficient. This paper focuses mainly Data scheme which focuses on using Advanced Encryption Standard (AES) for storing data securely and to perform fuzzy keyword searching on the encrypted data for retrieving the information .Therefore ,the wildcard-based technique is proposed which is the advanced fuzzy keyword search mechanism that returns the matching data based on similarity keywords semantics when users searching inputs exactly match the predefined keywords or the closet possible matching files, where exact match fails. The proposed solution focuses on making use of edit distance to quantify keywords similarity and to develop an efficient technique for constructing fuzzy keyword sets by reducing the storage and representation overheads.

Manish Kumar Yadav, Drishti Gugal, Shivani Matkar, Sanket Waghmare, [19] proposes a technique which uses fuzzy logic i.e the Encrypted Keyword Search in Cloud Computing using Fuzzy Logic. The scheme uses the basic approach so that the data confidentiality is maintained by encrypting the data. As the keywords are very vital information related to the files the data encryption scheme also demands the protection of keyword privacy . Thus, by encrypting the keywords it protects the keyword safety. The Fuzzy keyword search technique improves the serviceability of the system by matching the files perfectly or to the nearest possible files against the keywords entered by the user based on similarity. On entering keywords, this logic provides the user with encrypted keyword search in cloud, to receive best possible files in a more secured fashion, by protecting the privacy of user's documents.

Saumya Sharma, Amrita Bhagtani, Parth Agarwal, Ankit Mohite,[20] proposed N-Gram Fuzzy Keyword Search On Encrypted User Data in Cloud. In this paper, the different techniques which has been used for storing the data includes one storage server for storing the encrypted data, and various fuzzy keyword searching techniques like wildcard based and N (2) gram-based technique are considered and explained how the proposed model with 2 servers (security and storage server) and how N (2) gram fuzzy keyword search gives better accuracy than N(3) gram.We demonstrate encrypting and uploading of user files, downloading decrypted files, performing fuzzy search, and ensuring data security per user.

The following table 2.1 gives a summary of various papers that has been studied.

SR.NO	TECHNIQUES	DISADVANTAGES
1.	Wildcard Based Technique.	1. Needs large storage capacity as it generates so many fuzzy keywords from a given keyword . 2. Hashing unsuitable because order not preserved.
2.	Single Keyword Searching.	1. Support only exact keyword searching . 2. Cannot be used to search over large data set.
3.	Multi-Keyword Search.	1. Does not support semantic search.
4.	Ranked Keyword Search.	1. Efficient when it is used with multi-keyword techni
5.	Fuzzy Keyword Search.	1. It is hard to distinguish many confusing pairs of wo typos or different words.

Table.1 Summary of Literature Survey

III. EXISTING SYSTEM

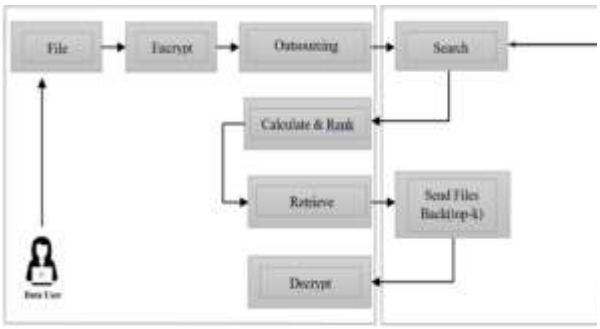

Figure.1 Block Diagram of Existing System

Disadvantages of Existing System:

- It still not adequate to provide users with acceptable result ranking functionality.
- Computational overhead on user's side for calculating the rank.
- It cannot accommodate such high service-level requirements like system usability, user searching experience, and easy information discovery.
- Do not get relevant data.
- Less efficient.

IV. PROBLEM STATEMENT

In the proposed architecture, it is required to follow the security definition deployed in the traditional searchable encryption when fuzzy keyword search scheme is used . More important thing is nothing should be leaked from the files which is remotely stored and the index beyond the outcome and the pattern of search queries. The drawback of efficient and privacy-preserving fuzzy keyword search services over encrypted cloud data is addressed in this scheme using N-gram technique.

Specifically, we have the following goals:

1. To examine the different mechanisms for building storage-efficient fuzzy keyword sets.
2. To develop and design the efficient and effective fuzzy search schemes which are based on the constructed fuzzy keyword sets.
3. To verify and validate the security and to assess the performance by conducting extensive experiments.

Therefore, the idea behind the proposed system is to quantify keywords' similarities and build an advanced technique for creating fuzzy keywords and then correlating them with the already stored n-grams from the cloud database [25]. Thus, the keywords are stored in an encrypted format in the database, the users' keyword is also encrypted and then matching them onto the cloud. The main aim of the scheme is to provide the security of data for every user.

V. PROPOSED SYSTEM

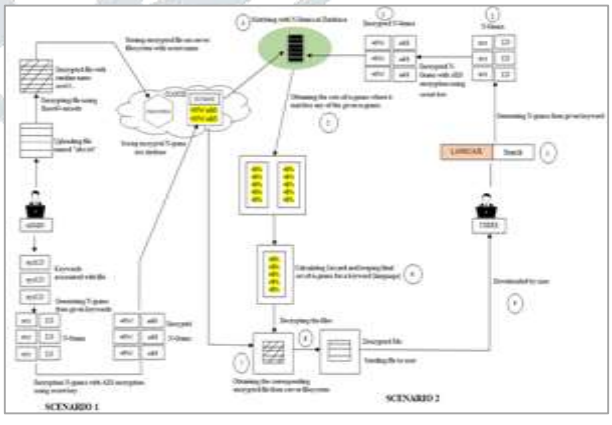

Figure.2 Block Diagram of Proposed System

A. ALGORITHM USED

SCENARIO 1: ADMIN

Step 1: Data owner uploads a file.
Step 2: Encrypt file using base 64 encode and upload the file in cloud server filesystem.

Else if filename already exists.
Overwrite

Step 3: Generate keywords associated with the file.
Step 4: Generate N-Grams from given keywords.
Step 5: Encrypt N-Grams with AES encryption.
Step 6: Store the encrypted N-Grams in cloud server database.

SCENARIO 2: USER

Step 1: Input keyword to the system for searching.
Step 2: Encrypt user filename and generate N-Grams.
Step 3:Encrypt N-Grams using AES algorithm and upload the encrypted N-Grams mentioned by the logged in user in database table.
Step 4: For every encrypted N-Grams of the keyword. Compare the encrypted N-Grams with the first table (i.e index 0)

If found
Add this to the set of N-Grams
Else continue.
End For

Step 5: Display the final set of N-Grams for the keyword using Jaccard coefficient.
Step 6: Decrypt the file and send to user.
Step 7: Download the file.

B. METHODOLOGY

***N-GRAM GENERATION*:**

1. Suppose we have to store keyword:"december".
2. N-grams: dec ece cem emb mbe ber.
3. Encrypted n-grams: htr yu6 ft5 5ty kl3 err.
4. Store htr into index_0 table (1st table).
5. Storing yu6 into index_1 table (2nd table).
6. Storing ft5into index_2 table (3rd table).
7. Storing 5ty into index_3 table and so on….
8. All n-grams are stored into single table i.e like we are storing the first n-gram in first table, second n-gram in second table and so on.
9. The process will reduce the number of comparisons required to match the n-grams and hence faster the search results.

JACCARD COEFFIEICNT CALCULATION:

The Jaccard index is used to find the similarity between the set of keywords in the set.

The formula to find the Index is: $\mathbf{J(A,B)} = \frac{|\mathbf{A} \cap \mathbf{B}|}{|\mathbf{A} \cup \mathbf{B}|}$

If A and B are both same, we define J(A,B) = 1 and 0 when they are disjoint i.e 0 ≤ J(A,B) ≤ 1.

Example:

A= Flunk	B = Flunker
N-grams for N=2:	N-grams for N=2:
Fl , lu , un, nk	Fl, lu , un ,nk , ke , er

J(A,B) = |A ∩ B| / |A ∪ B| = 4/6 = 0.666 = 0.7 = 70% Match

VI. ADVANTAGES

- The proposed scheme can efficiently handle spelling mistakes, typos.
- In the proposed schemes it introduces low overhead on computation and communication.
- It enables authenticated data users to achieve secure ,convenient and efficient searches over multiple data owner's data.
- The results are accurate enough to get exact files searched by the user.

VII. CONCLUSION

The proposed scheme provides a method of searching based on the keyword defined by the user. By using the N-gram based technique we get a wider set of data for the fuzzy pattern search which we then present to the user which increases the system efficiency and helps in the whole system being well organized and systematic. And with the help of including two algorithms AES 256 and Base64 the privacy is conserved which ensures that all comparisons and fetching of data is done in a way that the data is always protected at every moment of time.

REFERENCES

[1] Deepali D. Rane and Dr.V.R.Ghorpade " Multi-User Multi-Keyword Privacy Preserving Ranked Based Search Over Encrypted Cloud Data" International Conference on Pervasive Computing (ICPC), 2015.
[2] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. of ICDCS'10, 2010.
[3] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS, 2005.
[4] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of S&P, 2000.
[5]Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE, and Qian Wang, Member, IEEE "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL., NO.1,2015.
[6] Bing Wang, Wei Song, Wenjing Lou, and Y. Thomas Hou "Inverted Index Based Multi-Keyword Public-key Searchable Encryption with Strong Privacy Guarantee" IEEE Conference on Computer Communications (INFOCOM), 2015.
[7] Yanzhi Ren, Yingying Chen, Jie Yang, Bin Xie "Privacy-preserving Ranked Multi-Keyword Search Leveraging Polynomial Function in Cloud Computing" Globecom Communication and Information System Security Symposium 2014.
[8] Hongwei Li, Dongxiao Liu,Yuanshun Dai, Tom H. Luan, And Xuemin (Sherman) Shen "Enabling Efficient

Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage", December 2014.
[9] Mikhail Strizhov and Indrajit Ray "Multi-keyword Similarity Search Over Encrypted Cloud Data" International Conference on Pervasive Computing (ICPC), 2012.
[10] E.-J. Goh, "Bloom filters in order to construct the indexes for the data files" IEEE Conference on Computerer Communications 2016.
[11] Jun Zhou, Zhenfu Cao, Xiaolei Dong and Xiaodong Lin "More Efficient Verifiable Outsourced Computation from Any Oneway Trapdoor Function" IEEE ICC - Communication and Information Systems Security Symposium, 2015.
[12] Fanyu Bu, Yu Ma, Zhikui Chen and Han Xu "Privacy Preserving Back-Propagation Based on BGV on Cloud" 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), and 2015 IEEE 12th International Conf on Embedded Software and Systems (ICESS).
[13] Joseph K, "Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud" 2015. [14] Zhangjie Fu, Member, IEEE, Jiangang Shu, Xingming Sun, and Nigel Linge "Verifiable Keyword-based Semantic Search over Encrypted Cloud Data" IEEE Transactions on Consumer Electronics, Vol. 60, No. 4, November 2014.
[15] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. of IEEE INFOCOM'10 Mini-Conference, San Diego, CA, USA, March 2010.
[16] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. of EUROCRYPT, IEEE Conference on Computer Communications 2004.
[17] Utkarsh Joshi, Neeraj Vishwakarma , A.Murugan "Fuzzy Keyword Search over Encrypted Data" in International Journal of Innovative Research in Science, Engineering and Technology Vol. 6, Issue 4, April 2017.
[18] Dr.Narendra Shekokar , Kunjita Sampat, Chandni Chandawalli ,Janvhi Shah "Implementation of fuzzy keyword search over encrypted data in cloud computing" in ICACTA-2015.
[19] Manish Kumar Yadav, Drishti Gugal, Shivani Matkar, Sanket Waghmare "Encrypted Keyword Search in Cloud Computing using Fuzzy Logic" in IEEE Xplore 2019.
[20] Saumya Sharma, Amrita Bhagtani, Parth Agarwal, Ankit Mohite[20] "N-Gram Fuzzy Keyword Search On Encrypted User Data in Cloud" in International Journal of Open Information Technologies 2017.
[21] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. of ICDCS'10, 2010.
[22] Ms. Jabeen Akkalkot , Ms. S. Shanmug Priya, "A survey on keyword based search mechanism for data stored in cloud," in Proceedings of International Journal of Computer Science and Mobile Computing. ACM, May- 2016, pg. 235-240.
[23] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS, 2005.
[24] JianLi,Ruhui Ma, HaibingGaun, "TEES: An Efficient Search Scheme Over Encrypted data on Mobile Cloud" IEEE Transactions on Cloud Computing, TCC 2015.
[25] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposium on Security and Privacy'00, 2000.