Cloud Data Security Using Group Multi-Keyword Top K Similarity Search Using Asymmetric Encryption

Ms. Khuspreet Kaur, Dr. Meenakshi Bansal

Abstract: Cloud computing is a kind of area which has opened new doors to everyone.This allows for new types of services where online computing and network resources are available. Anyone who want to use it can pay and use online service. One of cloud computing most popular services is data outsourcing. Both public and private organizations can now outsource their large amounts of data to the cloud for cost and convenience reasons and enjoy the benefits of remote storage and management. At the same time, a major concern is the confidentiality of data stored remotely on untrusted cloud servers. To reduce these concerns about sensitive data such as personal health records, emails, income tax and financial reports, which are usually outsourced using well-known cryptographic techniques in encrypted form. Although encrypted data storage protects remote data from unauthorized access, it obscures some basic but essential data use services such as searching for plaintext keywords. For the encrypted data used by AWS and Google Cloud, a lot of techniques are used. Like Searchable encryption, you can store encrypted documents on a remote, honest but curious server, and query that data on the server itself without having to decrypt documents before searching. Not only does this protect the data from the server's prying eyes, but it can also reduce the overhead communication between the server and the user and the latter's local processing.

Index Terms: Group multi-keyword search, Asymmetric SE scheme, Cloud computing, Data encryption, random traversal, multi-keyword top-k search.

1 INTRODUCTION

Cloud computing is a modern computing paradigm in which data owners outsource their data to cloud storage and has emerged as a revolutionary phenomenon in both IT industries and science communities with a number of prominent features such as high scalability and pay-as-you-go stylethat made it possible for cloud consumers to purchase powerful computing resources as services according to their needs, so cloud users no longer have to worry about the complexity of hardware platform management.Through exporting data files into the cloud, it offers large companies as well as individual users many advantages because they can dynamically increase their storage space as and when necessary without purchasing any storage devices (Armbrust et al., 2009). i.e.

(1) Users can at any time, from anywhere, access the remotely stored data and allow approved users to share the information.

(2) Users can be freed from the local storage management burden.

(3) Avoiding capital spending on the cost of hardware and software, etc.

A variety of cloud storage services have been available date, such as Amazon Simple Storage Space (S3), Rack Space, Google, Microsoft, etc. By addition, all of these outsourced data advantages by cloud, there are a number of significant issues.

One of the major issues is the privacy of outsourced cloud data, i.e. sensitive information such as e-mail, health records, and government data may leak or even be hacked to unauthorized users. Because the cloud is an open platform; it is the target of both malicious insiders and outsiders attacking. Usually, cloud service providers (CSPs) provide data security through mechanisms such as virtualizations and firewalls. However, due to remote cloud storage servers, these mechanisms do not protect the privacy of users from the CSP itself. A natural approach to sensitive data privacy is to encrypt data before outsourcing it to the cloud and recover data via keyword-related search over encrypted data. Although encryption protects against unauthorized access, it significantly increases data owners ' overhead computing particularly when they have resource-constrained mobile devices and large data file sizes. Cloud computing framework is an encouraging new innovation & incredibly fastens the advancement of the extensive gauge information stockpiling, handling and dispersion. Security and protection wind up to be the real worries when information owners 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. And, in recent years, several Searchable Encryption (SE) schemes have been introduced to allow searching over encrypted data. The SE solutions include creating an archive that can be searched in such a way that information is shielded from the remote cloud server while allowing searching for documents.The index is a data structure that keeps track of a stored document set while facilitating an effective keyword search, i.e. the index returns a pointer to the documents containing the keyword given a keyword. Such solutions vary as they allow searching for single keywords or multi-keyword searches and types of

- *Kushpreet Kaur is currently pursuing masters degree program in Computer Science and Engineering in Yadawindra College of Engineering, Punjabi University, Talwandi Sabo, PH-9478906966. E-mail: kushiwander16@gmail.com.*
- *Dr. Meenakshi Bansal is a Supervisor currently working Assistant Professor in Computer Science and Engineering in Yadawindra College of Engineering, Punjabi University, Talwandi , PH-8146800408. E-mail: author_ermeenu10@gmail.com*

(This information is optional; change it according to your need.)

techniques used to create the search query.Some of them make the notion of looking for similarities. The problem of similarity search consists of a collection of data items characterized by certain features, a query specifying a value for a particular feature, and a similarity metric to measure the relevance between query items and data items.Nonetheless, either these techniques do not permit searching for numerous keywords and rating retrieved documents in terms of similarity ratings, or they are very intensive in computational terms.

2. PROBLEM STATEMENT

2.1 Existing system

So Goh et al. came up with the searchable Symmetric encryption (SSE) and provided a safe keyword search based on the pseudo-random functions and the Bloom filters, but the time cost of the Goh scheme was O(n). Song et al. defined the problem of searching the encrypted data on the cloud server and proposed a searchable encryption scheme symmetric algorithm. Curtmola et al. then implemented SSE's two formal concepts and provided an inverted list-dependent approach to boost query efficiency, which proved to be more effective than the other works. Most of the study, however, tested only the single keyword Boolean search aid, which was not sufficiently advanced to accommodate complex features.As a result, several works have been proposed in recent years to accomplish various types of complex queries such as searching for similarities, searching multi-keywords, etc.

2.2 Limitations of Existing System

Usually large costs in terms of data usage are incurred by applying these solutions to data encryption, which makes conventional data processing methods work well over encrypted data. The same key is used in this system to secure the data trapdoor; the one that is vulnerable to unauthorized access. The time-complexity of trapdoor creation is high. Most of these approaches cannot simultaneously experience the high search efficiency and strong data protection, mostly when applied to large data authentication, which presents high scalability as well as the challenges of performance. The structure is shown in figure: 1.

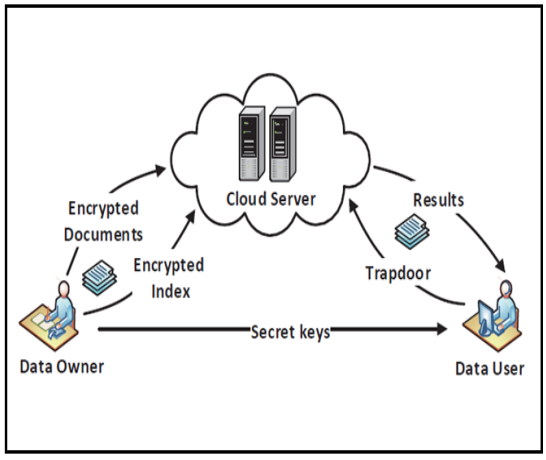

Fig.1: *Top-k search over encrypted data[16]*

2.2 Proposed System

Asymmetric encryption is used in the proposed system to encrypt the data rather than symmetric encryption. The proposed design of the device shown in figure 2

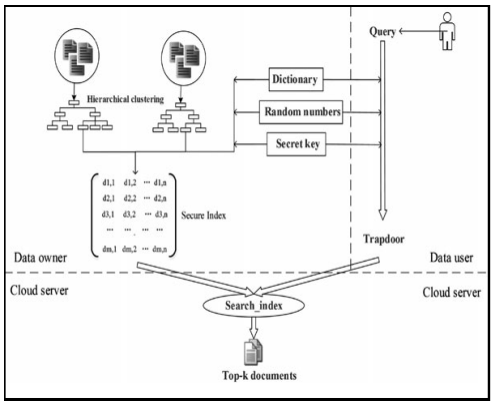

Fig. 2: *Proposed System*

In addition, proposed architecture is based on the hierarchical cluster and facilitates top-rank search over encrypted data in order to increase the request efficiency and information usefulness using the Team Multi-Keyword Top-k Search Scheme (GMTS). In this system, the cluster splits the sub-cluster in the dictionary and creates a searchable index for individual cluster. For instance, using the Random Traversal Algorithmic Program (RTRA) in order to improve the data security, wherever an owner generates a hierarchical cluster as the searchable index and assigns the random key to index, that the data user would assign a random key to each document. In the proposed system peer to peer architecture is used to improve the efficiency of communication between the user and owner.

3. METHODOLOGY

In this section existing system methodology using symmetric encryption and proposed system methodology using asymmetric encryption id discussed.

3.1 Existing System Methodology

Symmetric cryptography: Symmetric cryptography is a cryptographic algorithm which is used to encrypt and decrypt the data with same key. It is also known as secure key algorithm. Data Encryption and Decryption: Encryption is a type of security that converts unreadable plain text, images or other information into cipher text. The transformation of encrypted data as text or image into its original form is called decryption. It is generally a reverse process of encryption. It decodes the encrypted information with secret key so that an authorized user can decrypt the data and read the data.

Symmetric Algorithms: There are two types of symmetric algorithms:

- Block algorithms: The plain data is converted into encoded bits of electrical information with a particular length. The data is encrypted using a secret key. The system keeps the data in its memory as it waits for complete blocks as the data is encrypted.

- Stream algorithms. Data is encrypted as it streams rather than being stored in the memory of the system.

In figure 3 flow of existing system have been shown:

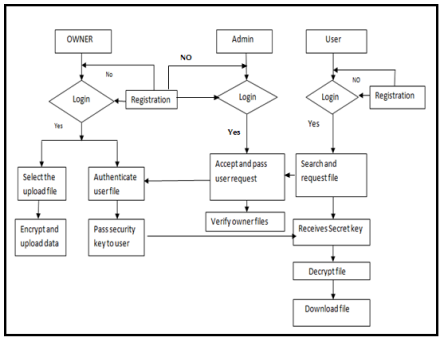

Fig.3: *Flowchart of Existing System*

3.2 Proposed system methodology

Asymmetric cryptography

In asymmetric cryptography, data is encrypted and decrypted using public and private keys. With everyone, one key can be shared; it's called the public key. The other key is kept as a secret; the private key is named. Any key either public or private can be used for encryption the message.Message will be decrypted using key other than that used for encryption.

RSA asymmetric Algorithm

RSA algorithm is an asymmetric algorithm for cryptography and is used with two different keys to encrypt and decrypt the data. i.e. Public and Private Key. As the title explains everyone being given the Public Key and Private Key being kept private.

Algorithms for Proposed System as shown in figure 4:

A. Select file:to selects the document file which uploads on cloud server.

B. key Generation:

1. Generate the public key using RSA.
2. Set the key size.
3. Generate the private key.

C. Encryption: Encrypt the file using RSA algorithm and upload the file on cloud server.

D. Keyword based search: Searching the file on cloud server using keyword or index.

E. Decryption: Decrypt the file using private key and download the file.

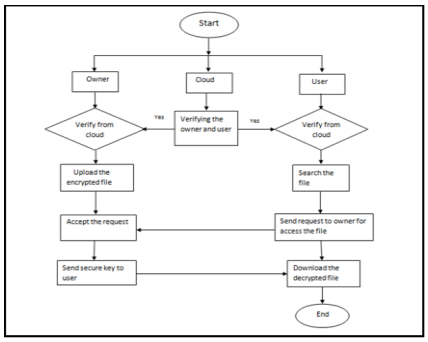

Fig.4: *Flowchart of proposed system*

Tools used

- System: Pentium Dual Core
- Ram: 1GB.
- Operating system: Windows 7, 8.1,10.
- Coding Language: HTML,CSS,PHP
- Tool: NOTEPAD++
- Platform web server : XAMPP
- Database: MYSQL

4. IMPLEMENTATION OF THE PROPOSED SYSTEM

Proposed system is a secure communication system where owner upload the encrypt data on cloud server and that data access by user using private key. There are four modules:

Modules

- Data owner
- Cloud server
- Search user
- Peer to Peer Communication

4.1 Working of system

Cloud admin panel

In this panel, all work is depending on server who is verifying all user accounts which registered on cloud and provide the authenticity to that account. Cloud admin also gives the rank to each file which is stored in cloud after encryption by their owner.

a) Working of cloud admin

- **Login panel of cloud admin:**
  In login panel, Admin can login using their specific username and password which is generatedstatically. After login, opens the dashboard of admin where admin can perform various actions such as view all the user and owner who are registered in server and also verify the user and gives the rank on encryption files which is uploaded on server
- **Activate User**
  In Admin s dashboard, one can see all the user and owner and user who are registered and verify and gives the authorization to each one. Send the secure activate key to owner and user so that they can securely access their account and become an authorized.
- **Secure activate Key**
  After generate the activation key, admin send the secure activate key to owner and user via mail on that email id which is entered at the time of registration. Each user has specific key to activate their account and this key helps to generate one-time key for one person.
- **Verify files**
  After uploads the files on cloud server admin gives the rank to each file which is display on admin's dashboard. Admin gives the rank to each file as per files specification no. of searching and no. of requests.

b) Owner Panel

In this panel all work are depend on owner such as select and encrypt the file and upload that file on cloud server and

owner also accept the request which is send by user for private key and send the private key.

Working of owner panel

- **Registration Form**
  Owner can be register on registration page before going to be login. In this section, owner fill their basic information such as user name, address, and password, confirm password, email address, mobile number and type means you are user or owner etc. After that, they click on register button to register their details which is shown on server's dashboard for verification.

- **Login panel of owner**
  In login panel, owner can be login their account by using their specific username and password which is generated after registration. After login, the dashboard opens where the owner can perform various actions such as activate the account using key, choose the file and encrypt that file before uploading, then upload the file on server and also see all request which is sent by user for access of the files.

- **Activate Account**
  Owner activates their account using the secure key which is sent by admin via mail which the owner fills in the registration form. Owner without activating their account cannot use their dashboard for further actions such as upload encrypted files.

- **Upload file**
  Choose the file which is upload on cloud server as well as given the identification id (f_id), subject and keyword to that file before encrypting the file.
  F_id =int(100),
  Sub=verchar(100),
  Keyword=verchar(100).

- **Encryption**
  Encrypt the selected directory to the cloud server before uploading. Use an asymmetric RSA algorithm in the back end of the system to encrypt the original text into cipher text using the public key.

- **Secure File**
  All requests are display on owner's dashboard which is send by users for private key and owner view the details of user such as name of user who wants the private key and the name of that file which files user want to access.After that owner accept the request of users and send the secure key to user via mail.

- **Secure key**
  Owner send the secure private key to user and that key generate on the spot when owner wants to send the key to user and this private key generatesone-timekey for one user without store in database. Owner sends this secure private key via mail to user.

c) User Panel

In this panel all work is dependent on user such as on the database search file and send the request to the owner to access the file and decrypt the file using the private key and this key is obtained by the user through the owner.

Working of user panel

- **Registration Form**
  User can be register on registration page before going to be login. In this section, user fill their basic information such as user name, address, password, confirm password, email address, mobile number and type which means you are user or owner etc. After that, they click on register button to register their details which is shown on server's dashboard for verification.

- **Login panel of User**
  In login panel, user can be login their account by using their specific username and password which is generates after registration. After login opens the dashboard of user where user can perform various actions such as activate the account using key, search the file and also send request the request to owner of that file for accessing purpose.

- **Activate User Account**
  User activates their account using the secure key which is send by admin via mail which is user fills in the registration form. User without activate their account cannot use their dashboard for further actions such as search the secure files.

- **Search Files**
  There are three methods of search the file on cloud server:
  Keyword based search: Users can search the secure file using the file keyword as a specification or file name given by the owner. For instance, user fills the keyword of file and all files of that name display on user's dashboard.

  Rank based search: Users can scan the protected folder using the file rank given to encrypted files by the administrator. For instance, user fill the rank 5 in search box then all files of five star display on user's dashboard.

  ID based search: User can search the secure file using the file id of the file which is given by owner to encrypted file. For instance, user fill the file ID in search box then the specific file which has that ID display on user's dashboard.

- **File Request**
  After search all files are display in user's dashboard and user choose the file and click on request button to send the request to owner of that file for private key so that they can access the file.

- **View file**
  User go to the dashboard and using the view section where display the file details like name of file, subject of file and click on view button to open the view file page then view the files after accept the request by owner and get the private key through owner which is used to decrypt the file.

- **Decryption**
  In decryption section, User uses that private key sent by owner via mail and through this key cipher text it converts data into original text. Without private key, the user cannot decrypt the data.

- **File Download**
  After decryption, the cipher data converted into original form and user can read the original file and after that user download the original file.

5. PERFORMANCE ANALYSIS

Performance is the model's entire correctness. It is calculated as the sum of each query's total load pages divided by the total number of pages p. It is as follows:

$$\text{Performance} = \frac{\text{Sum of total loading pages}}{\text{Total number of pages or queries}}$$

- **Access time**
  Access time is defined as the total time required by the server, owner and user to complete the process. In this process we use a number of pages such as login page, upload, verify file, search and request and view the file. The total access time to load the server and time taken to overall working process is 21.67s as compared to existing system which takes 26.18s as shown in figure 5

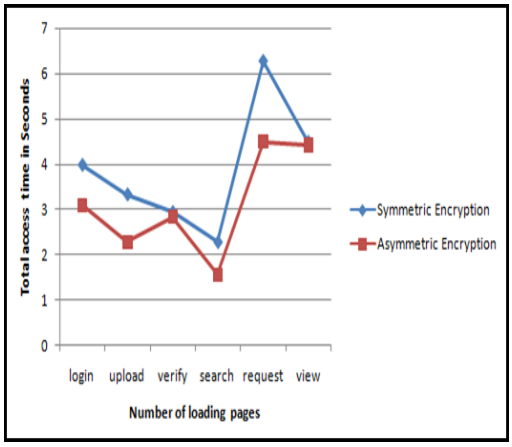

Fig. 5: *Access time*

- **Encrypted Time**
  The encryption time is defines as the total time which is used to select the file by owner which is need to upload then encrypt the file before before uploading on server . In proposed system, system take lass time to encrpt the data as compared to existing system because of asymmetric algorithm.

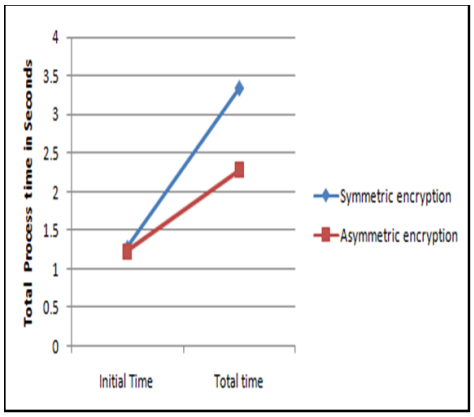

Fig. 6: *Encrypted time*

The total time existing system takes to encrypt the file is 3.34s whereas the proposed system takes less time that is 2.28s to encrypt the fileas shown in figure 6. RSA algorithm's time efficiency is less compared to other encryption algorithms, which is why the proposed system takes less time to encrypt the data compared to symmetric encryption.

- **Search time**
  Search time is defined as the total time which is used by user to search the secure file. In proposed system, using a hierarchical cluster based searching where the file subject is divided into subparts such as keyword, rank and the ID of file. In proposed system, the file can be searched by using their keyword and rank on server but in existing system, file search only by using the keyword of file.

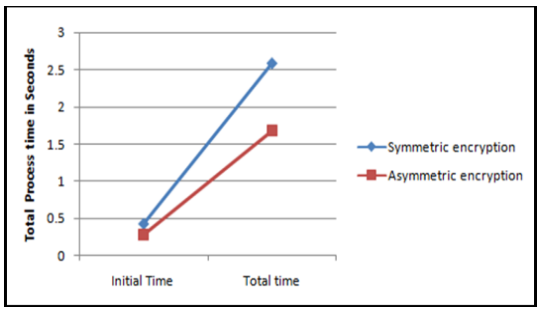

Fig. 7: *Search time*

The server takes the overall time 1.68s to search the data as well as provides the accurate resultsand existing system takes 2.58s to search the secure data on cloud server as shown in figure 7. Proposed system takes less time to search because in this system user search the data by specific id of that file that is unique id of that file.

- **Key generation time**
- Key generation time is defined as the total time which is involved to send request by user to owner,

accept the request by owner and also send the secure key to user.Key generation process takes too much time for the reason that this system has used tri-communication which involved cloud, owner and user communication whereas proposed system used peer to peer communication between owner and user.

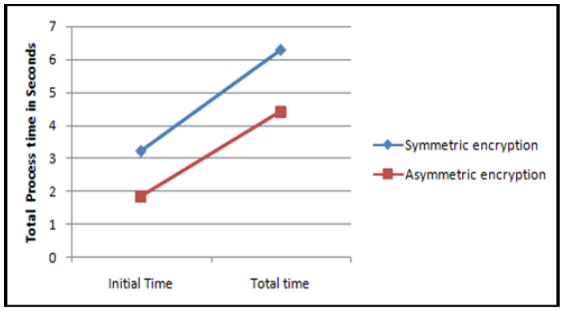

Fig.8: *Key generation time*

The total time server for generating the private key and sending it to the user is 4.41s. While the existing system takes longer time to generate and send the secure key to the user. As shown in figure 8, it takes about 6.28s.

- **Decryption time**
  The decryption time is defined as the total time used by a private key to decrypt it. The overall time server taken for decryptionis 3.02s whereas in the existing system, the total time takes for decryption is 2.83s as shown in figure 9. In proposed system, system takes more time to decrypt as compared to existing system because of asymmetric algorithm. In asymmetric encryption, the size of chunk of cipher text is increased at the time of encryption so it takes more time to decrypt.

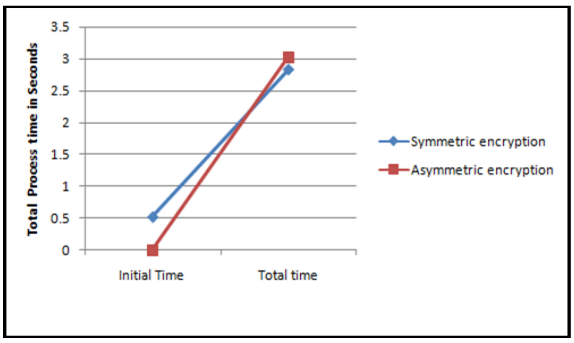

Fig. 9: *Decryption time*

Basically, the decryption time includes the overall decryption process as the user uses the private key in the secure key field that needs to be filled in and then clicks on the decryption button and then decrypts the data when the key matches the private key of the owner.

TABLE 1: *PERFORMANCE ANALYSIS OF PROPOSED SYSTEM V/S EXISTING SYSTEM*

Loading Pages	*Proposed System*	*Existing System*
Total Access Time	*21.67 seconds*	*26.18 seconds*
Encryption Time	*2.28 seconds*	*3.34 seconds*
Search Time	*1.68 seconds*	*2.58 seconds*
Key generation Time	*4.41 seconds*	*6.28 seconds*
Decryption Time	*3.02 seconds*	*2.83 seconds*

Proposed system takes less time to process as compared to existing system as shown in table no. 1. In existing system, search time and key generate process takes too much time because this system used tri-communication which involved cloud, owner and user communication whereas the proposed system used peer to peer communication between owner and user. Although proposed system takes more time to decrypt the data as compared to existing system because of the asymmetric encryption. In asymmetric encryption, the size of chunk of cipher text is intended to be increased at the time of encryption so it takes more time to decrypt. The average time which is used to each section in asymmetric encryption is 6.612 seconds whereas in symmetric encryption, the average time of each section is 8.242 seconds which is take more time as compared to proposed system.

6. FUNCTIONAL ANALYSIS

Functional Analysis provides systematic evidence that tested functions are available as specified by business and technical requirements, system documentation, and user manuals.

The following items are centered on functional testing:

Valid Input: It is necessary to accept defined groups of valid input.
Invalid Input: It is important to reject defined groups of invalid input.
Functions: It is necessary to exercise identified functions.
Output: It is necessary to exercise identified classes of application outputs.
Systems / Procedures: It is necessary to invoke interfacing systems or procedures.

Functional testing organization and preparation focuses on requirements, key functions, or special test cases. In addition, systematic coverage of business process flows must be considered for testing; data fields, predefined processes, and successive processes. Additional tests are identified and the effective value of current tests is determined before functional testing is complete.

5.2.3 System Analysis

System testing ensures that the entire integrated software system meets the requirements set out above. In order to ensure predictable and known results, it tests a configuration. The configuration-oriented system integration test is an example of system testing. System testing is based on descriptions of processes and flows, emphasizing pre-driven process links and points of integration.

7. CONCLUSION

This project depicts the successful implementation of search as well as uploads the encrypted and decrypted the data in cloud server using asymmetric cryptography. The user experiences faster data encryption and decryption without much involvement of the cloud server. This shows that the asymmetric search scheme algorithm has been more secure than symmetric encryption. It gives better security of data from the unauthorized access. This application assures secure end to end search and transfer the data without any error. We have therefore proposed the issue of multiple keywords ranked search over encrypted cloud data and building a variety of security requirements. We selected the effective principle of coordinate matching from a number of multi-keyword concepts. Firstly, it has been proposed to have a secure inner data computation. We also tried to achieve an efficient ranking result using the technique of k-nearest neighbor. This system works on a single cloud at the moment. It can be extended to sky computing in the future and provide improved security in multi-user systems.

FUTURE WORK

In future, the work may be extended by developing a stronger encryption algorithm with high efficiency and less memory usage. Another interesting topic to be discussed is the design of highly scalable searchable encryption to allow efficient searching of large functional databases.

8 .REFERENCE

[1] Song, D. X., Wagner, D., &Perrig, A. (2000). Practical techniques for searches on encrypted data. In Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000(pp. 44-55). IEEE.

[2] Seth, S. M., & Mishra, R. (2011). Comparative analysis of encryption algorithms for data communication 1.

[3] Agrawal, M., & Mishra, P. (2012). A comparative survey on symmetric key encryption techniques. International Journal on Computer Science and Engineering, 4(5), 877.

[4] Mondal, B., Dasgupta, K., & Dutta, P. (2012). Load balancing in cloud computing using stochastic hill climbing-a soft computing approach. Procedia Technology, 4, 783-789.

[5] Liang, H., Cai, L. X., Huang, D., Shen, X., & Peng, D. (2012). An SMDP-based service model for inter-domain resource allocation in mobile cloud networks. IEEE transactions on vehicular technology, 61(5), 2222-2232.

[6] Orencik, C., Kantarcioglu, M., &Savas, E. (2013, June). A practical and secure multi-keyword search method over encrypted cloud data. In 2013 IEEE Sixth International Conference on Cloud Computing (pp. 390-397). IEEE.

[7] Mahmoud, M. M., & Shen, X. (2012). A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 23(10), 1805-1818.

[8] Cao, N., Wang, C., Li, M., Ren, K., & Lou, W. (2013). Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Transactions on parallel and distributed systems, 25(1), 222-233.

[9] Jung, T., Mao, X., Li, X. Y., Tang, S. J., Gong, W., & Zhang, L. (2013, April). Privacy-preserving data aggregation without secure channel: Multivariate polynomial evaluation. In 2013 Proceedings IEEE INFOCOM (pp. 2634-2642). IEEE.

[10] Yang, Y., Li, H., Liu, W., Yao, H., & Wen, M. (2014, December). Secure dynamic searchable symmetric encryption with constant document update cost. In 2014 IEEE Global Communications Conference (pp. 775-780). IEEE.

[11] Tayde, S., &Siledar, S. (2015). File Encryption, Decryption Using AES Algorithm in Android Phone. International Journel of Advanced Research in computer science and software engineering, 5(5).

[12] Saini, N., Pandey, N., & Singh, A. P. (2015, September). Enhancement of security using cryptographic techniques. In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) (pp. 1-5). IEEE.

[13] K SrinivasaRao ,Dr Y. Vamsidhar(2015). Privacy-preserving multi-keyword ranked search over encrypted cloud data.International Journal of Applied Sciences, Engineering and Management ISSN 2320 – 3439(4),51 – 56.

[14] Tang, J., Cui, Y., Li, Q., Ren, K., Liu, J., &Buyya, R. (2016). Ensuring security and privacy preservation for cloud data services. ACM Computing Surveys (CSUR), 49(1), 13.

[15] Ying, Z., Li, H., Ma, J., Zhang, J., & Cui, J. (2016). Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating. Science China Information Sciences, 59(4), 042701.

[16] Ding, X., Liu, P., & Jin, H. (2017). Privacy-Preserving Multi-Keyword Top-$ k $ k Similarity Search Over Encrypted Data. IEEE Transactions on Dependable and Secure Computing, 16(2), 344-357.

[17] Liu, C., Zhu, L., & Chen, J. (2017). Efficient searchable symmetric encryption for storing multiple source dynamic social data on cloud. Journal of Network and Computer Applications, 86, 3-14.

[18] Kisembe, P., &Jeberson, W. (2017). Future of Peer-To-Peer Technology with the rise of Cloud Computing. International Journal of Peer to Peer Networks (IJP2P), 8.

[19] Peng, T., Lin, Y., Yao, X., & Zhang, W. (2018). An efficient ranked multi-keyword search for multiple data owners over encrypted cloud data. IEEE Access, 6, 21924-21933.

[20] Ian H. Witten, Alistair Moffat, and Timothy C. Bell: Managing Gigabytes (2nd Ed.): Compressing and Indexing Documents and Images. Morgan Kaufmann Publishers Inc., 1999.
[21] ZvikaBrakerski: Fully homomorphic encryption without modulus switching from classical GapSVP. In Proceeding of the 32nd Annual International Cryptology Conference CRYPTO 2012, 2012.
[22] ZvikaBrakerski, Craig Gentry, and Vinod Vaikuntanathan: (Leveled) Fully homomorphic encryption without bootstrapping. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, 2012.
[23] ZvikaBrakerski, Craig Gentry, and Vinod Vaikuntanathan: Fully Homomorphic Encryption without Bootstrapping. Cryptology ePrint Archive, Report 2011/277, 2011.
[24] Yan-Cheng Chang and Michael Mitzenmacher: Privacy preserving keyword searches on remote encrypted data. In Proceedings of the 3rd International Conference on Applied Cryptography and Network Security, 2005.
[25] AshwinSwaminathan, Yinian Mao, Guan-Ming Su, Hongmei Gou, Avinash L. Varna, Shan He, Min Wu, and Douglas W. Oard: Confidentiality-preserving rank-ordered search. In Proceedings of the ACM Workshop on Storage Security and Survivability, 2007.
[26] RFC: Request for comments database. http://www.ietf.org/rfc.html, 2015.
[27] Bradford Nichols, Dick Buttlar, and Jacqueline Proulx Farrell: Pthreads programming. O'Reilly & Associates, Inc., 1996.
[28] Christoph Bösch, Pieter Hartel, Willem Jonker, and Andreas Peter: A survey of provably secure searchable encryption. ACM Computing Surveys, vol. 47, no. 2, pp. 1-51, 2014.
[29] Amos Fiat and Moni Naor: Broadcast encryption. In Proceedings of the 13th Annual International Cryptology Conference CRYPTO 1993, 1993.
[30] Dan Boneh and Mark Zhandry: Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. In Proceedings of the 34th Annual International Cryptology Conference CRYPTO 2014, 2014.
[31] Mark Zhandry: How to Avoid Obfuscation Using Witness PRFs. In Proceedings of the 13th IACR Theory of Cryptography Conference TCC 2016, 2016.
[32] Dan Boneh, Craig Gentry, and Brent Waters: Collusion resistant broadcast encryption with short ciphertexts and private keys. In Proceedings of the 25th Annual International Cryptology Conference CRYPTO 2005, 2005.
[33] Ryuichi Sakai and Jun Furukawa: Identity-based broadcast encryption. Cryptology ePrint Archive, Report 2007/217, 2007. [47] Cecile Delerablee, Pascal Paillier, and David Pointcheval: Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In Proceedings of the First International Conference on Pairing-based Cryptography, 2007.
[34] 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.
[35] 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.
[36] 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.
[37] A.Swaminathan, Y. Mao, G. M. Su, H. Gou, A. Varna, S. He, M. Wu, and D. Oard, "Confidentialitypreserving rank-ordered search," in Proc. ACM ACM Workshop Storage Security Survivability, Alexandria, VA, 2007, pp. 7–12.
[38] 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.
[39] 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.
[40] A.Selvanayagi, "Optimizing cloud gaming experience through map reducing", in Scopus, vol.118, No.18, pp.2621-2626, Feb.2018.
[41] S.Saravanan, R.Bharathi, "Enhanced privacy and usability multikeyword search scheme Over mobile cloud storage", in Scopus, vol.118, No.8, pp.2265-2272, Feb. 2018.
[42] M.Murugesan, "Secure data compression scheme in cloud environments with backup recovery scheme", in Scopus, vol.118, No.8, pp. 467-471, Feb. 2018
[43] S.P.Yazhini, S.Santhiya, "Reliability and Confidentiality based data storage in cloud using merkle hash tree technique", in Scopus, vol. 118, No.8, pp.793-797, Feb. 2018.
[44] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in Theory of Cryptography. Springer, 2009, pp. 457–473.
[45] 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.
[46] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.
[47] 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.
[48] C. D. Manning, P. Raghavan, H. Schutze ¨ et al., Introduction to information retrieval. Cambridge university press Cambridge, 2008, vol. 1, no. 1.

[49] S. Brin and L. Page, "The anatomy of a large-scale hypertextual web search engine," Computer Networks and ISDN Systems, vol. 30, no. 17, 1998.
[50] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Computational Science and Its Applications. Springer, 2008, pp. 1249–1259.
[51] D. J. Park, K. Kim, and P. J. Lee, "Public key encryption with conjunctive field keyword search," in Information security applications. Springer, 2004, pp. 73–86.
[52] 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.
[53] 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.
[54] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Distributed Computing Systems (ICDCS), IEEE 30th International Conference on, 2010, pp. 253–262.
[55] 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.
[56] M. Chuah and W. Hu, "Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data," in Distributed Computing Systems Workshops (ICDCSW), the 31st International Conference on, 2011, pp. 273–281.
[57] 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.
[58] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Data Engineering (ICDE), 2012 IEEE 28th International Conference on, 2012, pp. 1156–1167.
[59] Q. Lv, W. Josephson, Z. Wang, M. Charikar, and K. Li, "Multiprobelsh: Efficient indexing for high-dimensional similarity search," in Proceedings of the 33rd International Conference on Very Large Data Bases. VLDB Endowment, 2007, pp. 950–961. X. Yuan, H. Cui, [60] X. Wang, and C. Wang, "Enabling privacyassured similarity retrieval over millions of encrypted records," in European Symposium on Research in Computer Security. Springer, 2015, pp. 40–60.