Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 11423 - 11438
Received 05 March 2021; Accepted 01 April 2021.

Multi-Keyword Similarity Search Using Asymmetric Encryption

K. Madan Mohan
Asst.Professor, Dept of Computer Science and Engineering,
CMR Institute of Technology, Kandlakoya (V), Medchal (M), Hyderabad. Pin : 501401,TS.
Research Scholar, Dept of Computer Science and Engineering, JNTUH, Kukatpally,
Hyderabad,500085,TS.
Mail-id: madan.keturu@gmail.com

Dr. B V Ram Naresh Yadav
Associate Professor, Department of CSE,
JNTUH College of Engineering Jagtial(JNTUHCEJ),
Nachupally, Jagtial
bvramnaresh@gmail.com

Abstract: Cloud computing has become a new ground for 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 the most popular cloud computing services is data outsourcing. Many business organizations have already benefited a great deal from Remote Data Rooms. The major concern is the security of this data stored on remote untrusted cloud servers. There should be no concerns over personal health data such as emails, income tax and financial reports because of use of well-known cryptography to protect sensitive data such as that. Encrypted access to digital data makes search retrieval of information difficult. A lot of techniques are used for encrypted data used by AWS and Google Cloud. Besides Searchable encryption, you can store encrypted documents on a remote, unbiased server, and query that data on the server itself with no need to decrypt before searching. This way, client-side encryption is both safer and more cost effective than server-side encryption.

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

1 INTRODUCTION

Although cloud computing a potentially disruptive paradigm in both IT and science communities, it is important for us to keep a close eye on this future. Through exporting their data to the cloud, they do not need to get any expensive data storage devices (Armbrust et al., 2009). e.g.

(1) Users can access the data anywhere, from any place in the world;
(2) Users will be freed from the problem of local storage management.
(3) Should spend less on hardware and software.

There have been several types of hosting products, such as Amazon Simple Storage Service (S3), as well as Rackspace, Google, Microsoft, etc. There are a number of dangers associated with cloud outsourcing of outsourced data as well as security risks.

One of the major issues facing cloud computing is the security of private personal information such as e-mail, health records, and financial data. An open platform in the cloud is important in keeping secure. Usually, cloud service providers (CSPs) use virtualization and firewall mechanisms to provide security. However, one should note that these systems do not protect sensitive information from being hacked by cloud storage owners. Encrypting sensitive data before exporting it and searching it using keyword-related encryption is a good way to preserve data privacy. Although encryption protects against unauthorized access, and this protects the owner from the risks, it raises considerable computing costs. Cloud Computing framework is an encouraging innovative innovation and extraordinarily quickens advancement of information stockpiling, handling and dissemination. Security and protection will be of the essence when data owners outsource data or information onto open cloud servers and are not within an administration department. To manage the spread of sensitive information, methodical steps should be taken first before transferring. Most of present works assume a single keyword inquiry without a positioning strategy. Searchable Encryption (SE) permits searching encrypted files. This new technique was introduced in the recent year. SE solutions include creating an archival system that is inaccessible from remote cloud servers while allowing search functions which are not tied to the cloud service. The index, of course, is used to find a specific document or to find a specific word. There are various kinds of search techniques used to create query, and they have a different result. Some of them find a commonality or relationship between things Similarity search problem describes a collection of data items characterized by certain features, a query with a specific value for a particular feature, and a similarity metric to measure the relevant relatedness. Needless to say, that those computational techniques are expensive in terms of time and money needed.

2.PROBLEMSTATEMENT

2.1 Existing system

Goh et al. developed the Symmetric encryption (SSE) and reduced the computational cost using Bloom filter, but the Go was difficult (n). Song et al. on the other hand described the problem of searching the encrypted data on the cloud server and devised a puzzle solving symmetric encryption algorithm. Thus Curtmola, et al. then introduced SSE's two formal principles to improve query performance. Most of the studies evaluated only the single keyword Boolean search techniques, which were not adequate enough to accommodate complex features. This means that diverse ideas have been presented in recent years to carry out different kinds of complicated queries.

2.2Limitations of Existing System

LuCC can face more costs when collecting ordinary data than when encrypting the data. The same device is used to encipher the trapdoor except the one that is unattainable to unauthorized entry. The construction of trapdoor is a time-consuming function. These approaches would not be applicable to the authentication and none of them can simultaneously provide the large-scale validation and security. The net profit is shown in the following figure: 1.

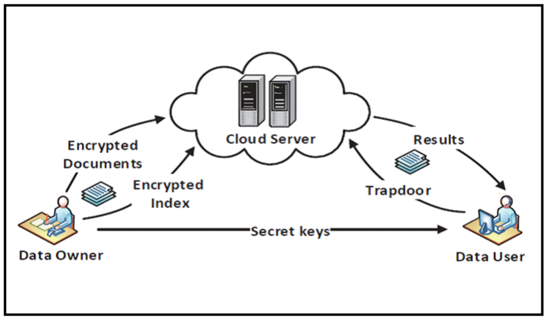


Fig.1: Top-k search over encrypted data [16]

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

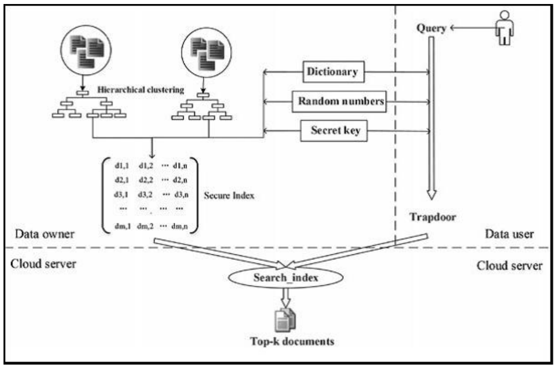


Fig. 2: Proposed System

In addition, proposed architecture is based on the hierarchical structure and ensures top-ranked search for databases using the team-keyword technique (GMTS). In this way, we will look for the contents of each individual cluster. For instance, if data owner uses Random Traversal Algorithmic Program (RTAP) to create the hierarchical index then the user is free to assign a random key to each document he wants to index. The proposed framework peer to peer design would achieve the efficiency of contact between users and the owners.

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 encryption is a kind of encryption algorithm which is used to encrypt and decrypt the data with same key. It is known as AES. Encryption is a sort of authentication that transforms unreadable text into a message in cipher text. Reading of encrypted messages is called decryption. It is a veritable decrypt. It will decrypt any encrypted information by using a secret key.

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.

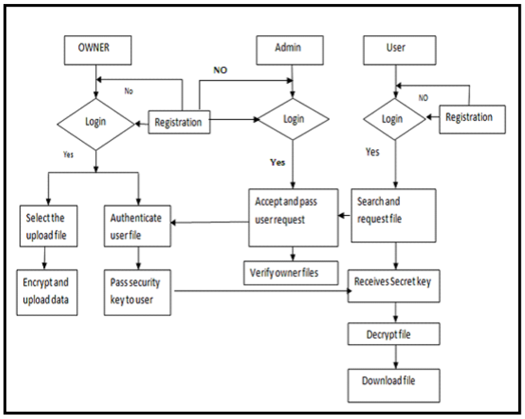


figure 3 flow of existing system have been shown:

3.2 Proposed system methodology

Asymmetric cryptography

In asymmetric cryptography, information is enciphered and deciphered using public and private keys. Everyone gets a public key. The other key is kept as a secret; the public key name is known. Either a private or public key may be used for encrypting the message. The message will be decrypted using the code which is different from the one used for encryption.

RSA asymmetric Algorithm

RSA algorithm is an asymmetric algorithm used to encrypt and decrypt data. e.g., Public and Private Key pair. This is "everyone being given Public Key and Private Key being kept private."
Algorithms for Proposed Systems 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.

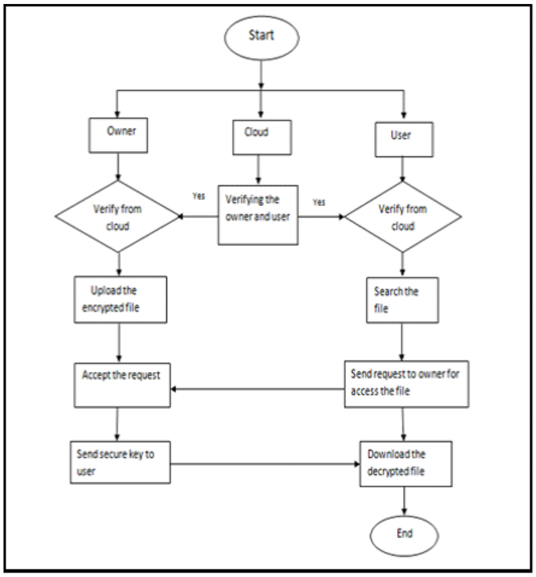

Start
Owner
Cloud
User
Verify from cloud
Yes
Verifying the owner and user
Yes
Verify from cloud
Upload the encrypted file
Search the file
Accept the request
Send request to owner for access the file
Send secure key to user
Download the decrypted file
End

Fig.4: *Flowchart of proposed system*

4.IMPLEMENTATIONOFTHEPROPOSEDSYSTEM

The proposed system is a secured electronic system where you can upload information and secure contact before it can be read. There are four modules in this course.

Modules

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

4.1 Working of system

Cloud admin panel

All work is based on a server that enforces all accounts on the cloud and guarantees validity of each account. This feature gives the rank to each file, which is stored in cloud by its owner.

a) Working of cloud admin

- **Login panel of cloud admin:**

In this way the Administrators will login using their own account login information. When admin logs in, a page lists all of the users and owners who are registered in the server, as well as their security access ranking.

- **Activate User**

In Admin; one can see which users are licensed, checked and allowed to exercise their privileges. Before granting permission to someone to access the owner's account, make sure that you give him an unlock key.

- **Secure activate Key**

An administrator sends out a secure activation key to the owner of the account and to each newly created user. Each user has a unique key to trigger their account and this key creates a single key for one person.

- **Verify files**

The rank of each file uploaded to the cloud server will be displayed on the dashboard of each admin. Administrator gives rank to file for searching and requests.

b) Owner Panel

In this panel all work is done by owner such as selecting file and encrypting the file. And the owner also approves the upload request and the uploader sends the key through email.

Working of owner panel

- **Registration Form**

Until registering, one must first visit the registration page. Owners supply some basic information such as user name, location, and password, confirm password, email address, mobile number, and gender. After that, they click the registration connection which appears on the dashboard to register their registration information.

- **Login panel of owner**

In the login screen, the owner will log into their account by entering their own username and password. The dashboard gives all the administrative power to the account holders.

- **Activate Account**

Owner unlocks their account using the safe key which is sent by the administrator using the mail which the owner fills in the form. Without accessing their account, subscribers cannot use their dashboard for more functions such as downloading encrypted data.

- **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.

- **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.PERFORMANCEANALYSIS

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:

Sum of total loading pages
Performance =

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

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 11423 - 11438
Received 05 March 2021; Accepted 01 April 2021.

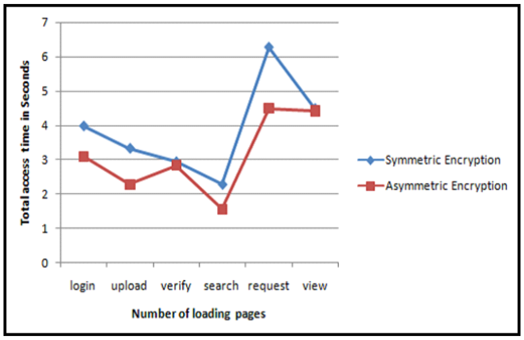


Fig. 5: *Access time*

- **Encrypted Time**

The encryption time is defining 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 encrypt the data as compared to existing system because of asymmetric algorithm.

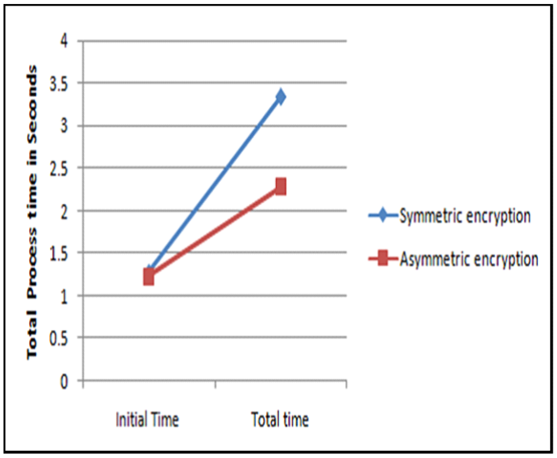


Fig. 6: *Encrypted time*

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 file as 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.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 11423 - 11438
Received 05 March 2021; Accepted 01 April 2021.

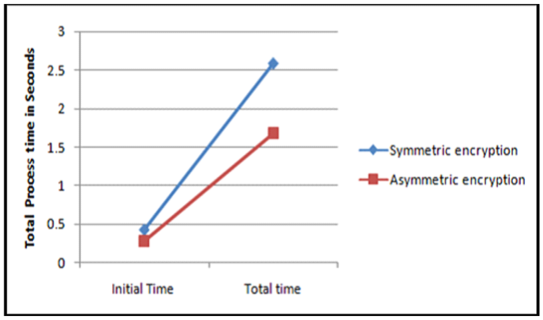


***Fig. 7:** Search time*

The server takes the overall time of 1.68 seconds to search the data and provides the accurate results, but it takes about twice the time of existing system to search data on the cloud server. The proposed system takes less time to search because this system searches the data by specific ids.

- **Key generation time**

It is measured in terms of the time of transfer from user to owner.
Accept and send the secure key to the user. In Key generation process, there is too much time because this system has used tri-communication, which involves cloud, owner and user communication, and proposed system, on the other hand, used peer to peer communication.

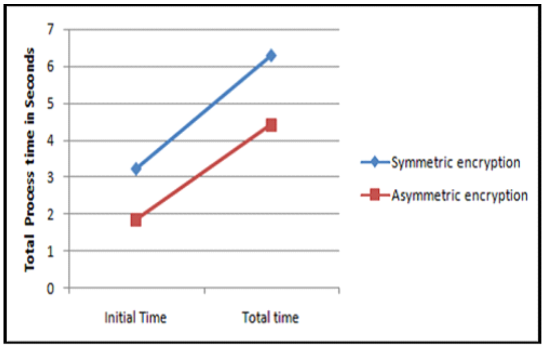


***Fig.8:** Key generation time*

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**

Decryption time is defined as the amount of time used by a private key to decrypt the cipher. Overall time taken for decryption in the LNU system is 3.02s compared to 2.83s in the existing system. New system uses more time for decryption as compared to current system because of asymmetric algorithm. During asymmetric encryption, the size of cipher text is increased gradually, so it takes longer to decrypt.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 11423 - 11438
Received 05 March 2021; Accepted 01 April 2021.

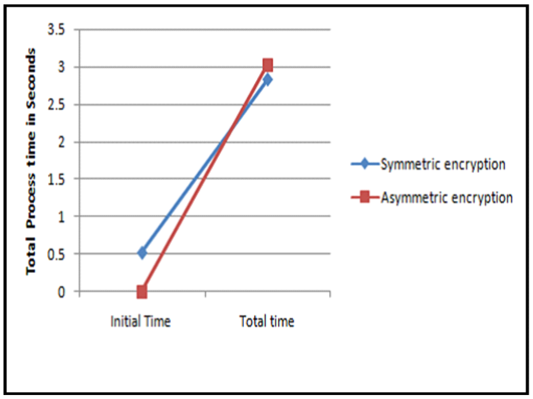
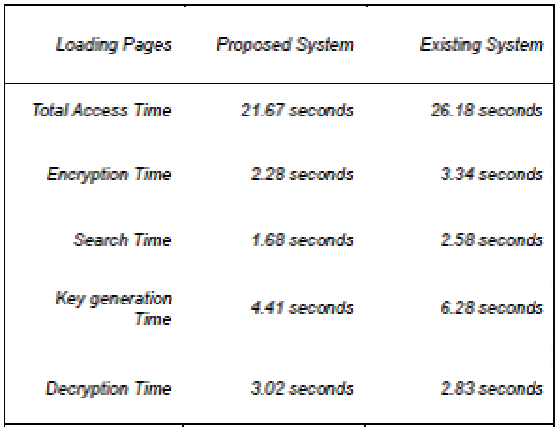


Fig. 9: *Decryption time*

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.

TABLE1: PERFORMANCEANALYSISOFPROPOSEDSYSTEMV/SEXISTINGSYSTEM



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*

The proposed system takes less time to process because of the reason that as shown in the table no. 1. In the existing system, search time and security keys take too much time due to communication between cloud and owner. The proposed system does have some advantages because it will take a bit longer time to decrypt the data. In asymmetric encryption, cipher text is intended to be made larger at the time of encryption, thereby taking longer to decrypt. The average time required for each section is higher in asymmetric encryption than that of symmetric encryption.

6.FUNCTIONALANALYSIS

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 cantered 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

The device checking ensures that there are no faults with the program. To develop an effective system, it tests a prototype. It's an example of checking in system configuration. System testing emphasizes process links and points of integration.

7.CONCLUSION

This project exemplifies efficient implementation of searches on an encrypted-decrypted cloud's server with public key cryptography. The consumer utilizes encryption methods without involving the cloud server. This indicates that asymmetric encryption has been more secure than symmetric encryption. It offers more efficient protection of valuable data because of improved encryption technologies. This software assures you fully safe data transfer and scan. We have concluded that keywords must be searched deciphered. We used the principle of coordination as a basis for designing our conceptual system. Firstly, it has been suggested that data facilities must be secured. We have tried a k-nearest neighbour technique to obtain a ranking result. This cloud storage system is currently running on a single server. This is useful in the future since sky computing is supposed to boost the security in multi-user systems.

FUTUREWORK

In the future, the work may be extended to optimize the algorithm with better efficiency, and less memory usage. Another important subject to be explored is the design of protection scheme that would allow efficient scanning of very large functional databases.

8. REFERENCE

[1] Song, D. X., Wagner, D., &Perrig, A. (2000). Practical techniques for searches on encrypted data. InProceeding 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. In2013 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. In2013 ProceedingsIEEE 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. In2014 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). Enhancementof security using cryptographic techniques. In2015 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 usableand 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. Brinand 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 Scienceand 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.