International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.271.01

Dynamic Secure Multi Keyword Rank based Search Algorithm

Priyanka Verma[1] Pawan Kumar[2]

[1]*Research Scholar, NIILM University, Kaithal*
[2]*Assoc. Professor, NIILM University, Kaithal*

Abstract - In order to study the performance of proposed Protected Hybrid Search (SHS) technique which is compared with the existing methods such as Enhanced semantic feature extraction (Term Frequency-Inverse Text Frequency) E-TFIDF and adaptively stable Searchable Symmetric Encryption (SSE) scheme. The output results are evaluated for certain parameters and the results are defined in table and graph values. In addition, the performance of the proposed SHS technique is checked using the following metrics such as precision, encryption and decryption speed, encryption and decryption time, file and keyword search time, token generation time and keyword storage. The proposed SHS technique is contrasted with existing methods such as Enhanced semantic feature extraction (E-TFIDF) method and Searchable Symmetric Encryption (SSE) Scheme.

Keywords: SHS, MRFHE.

I. INTRODUCTION

The proposed Modified Ring based Fully Homomorphic Encryption and Prim‟s (MRFHE-P) Algorithm is implemented with JAVA language. The simulation results are attained by using the CloudSim simulator. The proposed MRFHE-P Algorithm uses CACM dataset for performing dynamic multi keyword search on encrypted cloud data platform. The CACM dataset contains files such as cacm.all and query.text. The cacm.all file comprises of all queries related files and the query.text file comprises of user request queries. During the experiment conduction, the number of files is considered as the range of 50 to 500 and the number of keyword is considered as the range of 100 to 1000. Similarly, the size of document is considered from the 50 to 230 KB. The experiment evaluation is carried out using proposed Modified Ring based Fully Homomorphic Encryption and Prim‟s (MRFHE-P) Algorithm and existing methods such as Two-Round Searchable Encryption (TRSE) scheme implemented by Jiadi Yu et al. (2013) and adaptively secure Searchable Symmetric Encryption (SSE) scheme developed by Md Iftekhar Salam et al. (2015). The experimental evaluation of proposed MRFHE-P Algorithm is conducted on the following factor such as given below.

II. PERFORMANCE OF PROPOSED ALGORITHM

In order to examine the performance of Proposed Modified Ring based Fully Homomorphic Encryption and Prim‟s (MRFHE-P) Algorithm which is compared with the existing methods such as Two-Round Searchable Encryption (TRSE) scheme implemented by Jiadi Yu et al. (2013) and adaptively secure Searchable Symmetric Encryption (SSE) scheme developed by Md Iftekhar Salam et al. (2015). The tables and graphs are generated depends on the obtained performance values to prove the effectiveness of the proposed algorithm.

Search time for different keywords

The search time of the keyword is determined as the amount of time consumed to search the number of keywords present in a file. The search time of the keyword is mathematically expressed as given below.

$$KST = K_{ET} - K_{ST} \ldots \quad (5.10)$$

From the Equation (5.10), „*KST*‟ represents the searching time of keyword. Then, the keyword searching time is measured as the time difference between the ending time „K_{ET}‟ and staring time „K_{ST}‟ for searching the keyword in a file. The search time of the keyword is represented in milliseconds (ms). If the search time for different keywords is less, then the technique is said to be more efficient. To ensure user authentication, the proposed Safe Hybrid Search

(SHS) technique is implemented to perform protected hybrid search on encrypted cloud platform. The proposed SHS technique is performed during keyword search using the category-based indexing scheme, symbol-based tree traverse search scheme, gram-based search request and light weight multiple-to-many authentication protocol. The data owner must first store their encrypted files and index list on cloud platform. Generating a token to the keywords helps by comparing the search token and index list to retrieve the related document from the encrypted cloud setting. The cloud server uses the symbol-based tree traverse search scheme to ensure that the correct document is easily accessed with high privacy. The proposed SHS technique uses the light-weight multiple to many authentications protocol to secure the cloud data from unauthorized users when receiving the gram-based search request from the cloud user. The protection for cloud data is improved thereby.

Table 1.1 Results of search time for different files and keywords inRFHE-P algorithm

Search time for different Files (ms)				**Search time for different keywords (ms)**			
No. of files	**Existing TRSE scheme**	**Existing Adaptively secure SSE scheme**	**Proposed MRFHE-P Algorithm**	**No. of keywords**	**Existing TRSE scheme**	**Existing Adaptively secure SSE scheme**	**Proposed MRFHE-P Algorithm**
50	74	60	30	100	32	27	13
100	86	74	44	200	37	32	17
150	98	88	54	300	42	37	22
200	110	101	72	400	49	44	29
250	126	114	84	500	54	49	34
300	136	120	94	600	58	53	39
350	140	125	104	700	63	58	43
400	154	138	114	800	67	62	47
450	166	150	126	900	73	68	53
500	180	169	138	1000	79	74	59

The Table 1.1 demonstrates the performance of search time for different files and keywords. The simulation is carried out by comparing the proposed MRFHE-P Algorithm with existing methods such as Two-Round Searchable Encryption (TRSE) scheme implemented by Jiadi Yu et al. (2013) and adaptively secure Searchable Symmetric Encryption (SSE) scheme developed by Md Iftekhar Salam et al. (2015). While conducting the experiments, the number of file and number of keyword are considered from the range of 50 to 500 and 100 to 1000. As mentioned in Table 1.1, the searching time is gradually minimized by using three methods with respect to the different number of files and keywords. Comparatively, the proposedMRFHE-P Algorithm requires less time to search the files and keywords basedon the query request than the other existing methods. Then, the graph in belowfigures 1.1 and 1.2

are plotted depends on the values in Table 1.1 which is attained during the experimental conduction.

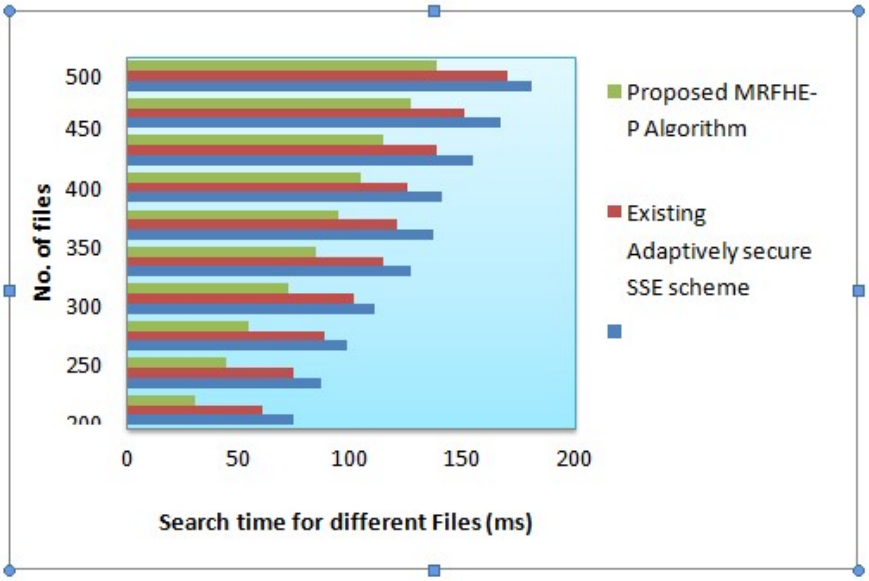

Figure 1.1 Measurements of search time for different filesin MRFHE-Palgorithm

The Figure 1.1 shows the performance results of search time for different files in the proposed MRFHE-P Algorithm, existing methods such as Two-Round Searchable Encryption (TRSE) scheme implemented by Jiadi Yu et al. (2013) and adaptively secure Searchable Symmetric Encryption (SSE) scheme developed by Md Iftekhar Salam et al. (2015). From the above Figure 1.1, it is clearly observed that, the proposed MRFHE-P Algorithm comparatively consumes less time taken to search the files which contain search keyword than the other existing methods. This is because, the proposed MRFHE-P Algorithm performs ranked based search for identifying the exact file which is related keyword to the search query request. Based on the ranking function, the file contain particular keywords are successfully ranked which makes the searching process becomes fast. Thus, the proposed MRFHE-P Algorithm reduces 35% and 27% time for searching the files when compared to Two-Round Searchable Encryption (TRSE) scheme implemented by Jiadi Yu et al. (2013) and adaptively secure Searchable Symmetric Encryption(SSE) scheme developed by Md Iftekhar Salam et al. (2015) respectively.

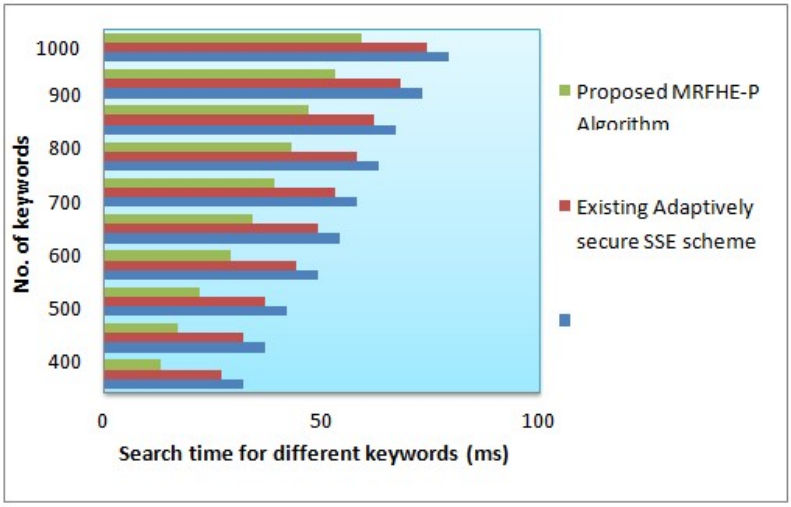

Figure 1.2 Measurement of search time for different keywords in MRFHE-P algorithm

The Figure 1.2 shows the performance results of search time for different keywords in the proposed MRFHE-P Algorithm, existing methods such as Two-Round Searchable Encryption (TRSE) scheme implemented by Jiadi Yu et al. (2013) and adaptively secure Searchable Symmetric Encryption (SSE) scheme developed by Md Iftekhar Salam et al. (2015). From the above Figure 1.2, it is clearly observed that, the proposed MRFHE-P Algorithm comparatively consumes less time taken to search the keywords which contain search keyword than the other existing methods. This is because, the proposed MRFHE-P Algorithm computes the keyword frequency of every files. According to the estimated keyword frequency, the keywords are sorted depend on ranks which helps to find the file hold related keywords. Thus, the proposed MRFHE-P Algorithm reduces 39% and 32% time for searching the keywords when compared to Two-Round Searchable Encryption (TRSE) scheme implemented by Jiadi Yu et al. (2013) and adaptively secure Searchable Symmetric Encryption (SSE) scheme developed by Md Iftekhar Salam et al. (2015) respectively.

III. CONCLUSION

The proposed Secure Hybrid Search (SHS) technique is introduced in order to perform secure hybrid search on encrypted cloud platform by ensuring the user authentication. During the keyword search, the proposed SHS technique is performed by utilizing the category based indexing, symbol based tree traverse search scheme, gram based search request and light weight many-to-many authentication protocol. At first, the data owner stores their encrypted files and index list on cloud platform. The generation of token to the keywords helps to extract the similar document from the encrypted cloud environment by comparing the search token and index list. The cloud server utilizes the symbol based tree traverse search scheme to ensure rapid access for finding the required document with high privacy. For protecting the cloud data from the unauthorized users, the proposed SHS technique uses the light weight many-to-many authentication protocol while getting the gram based search request from the cloud user. Thereby, the security to the cloud data gets enhanced.

REFERENCES

[1] Cheng Guo, Ningqi Luo, Md ZakirulAlam Bhuiyan, YingmoJie, Yuanfang Chen, Bin Feng and Muhammad Alam, 'Key-Aggregate Authentication Cryptosystem for Data Sharing in Dynamic Cloud Storage' , Future Generation Computer System, Elsevier, August 2017, pp. 1-30.

[2] Cheng-Kang Chu., Sherman S. M. Chow., Wen-Guey Tzeng, Jianying Zhouand Robert H. Deng,'Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage, IEEE Transactions on Parallel and Distributed Systems, vol.25, No. 2, February 2014, pp.468 477.

[3] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, 'Privacy-Preserving Public Auditing for Secure Cloud Storage', IEEE Transactions on Computers, vo1. 62, No. 2, February 2013, pp. 362 — 375.

[4] D. Chandramohan , T. Vengattaraman, D. Rajaguru and P. Dhavachelvan, 'A new privacy preserving technique for cloud service user endorsement using multi-agents', Journal of King Saud University - Computer and Information Sciences, Elsevier, vol. 28, No. 1, January 2016, pp. 37-54.

[5] Daniel Díaz-Sánchez, Florina Almenarez, Andrés Marín, Davide Proserpio, and Patricia Arias Cabarcos, 'Media Cloud: An Open Cloud Computing Middleware for Content Management', IEEE Transactions on Consumer Electronics, vol. 57, No. 2, May 2021, pp. 970-978.

[6] Deepa P L, S Vinoth Kumar and Dr S Karthik, Searching Techniques In Encrypted Cloud Data', International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) vol. 1, No. 8, October 2012, pp. 1-5.

[7] Guojun Wanga., Qin Liu., Jie Wub., Minyi Guo., Science Direct., Elsevier Journal., 'Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, Computers & Security, Elsevier, vol. 30, No. 5, July 2011, pp. 320-331.

[8] Gurpreet Singh and SupriyaKinger, 'Integrating AES, DES, and 3- DES Encryption Algorithms for Enhanced Data Security', International Journal of Scientific & Engineering Research, vol. 4, No. 7, July 2013, pp. 2058- 2062.

[9] Hongwei Li,Dongxiaoliu,Yuanshun Dai, Tom H. Luan and Xuemin (Sherman) Shen, 'Enabling Efficient Multi-Keyword Ranked Search over Encrypted Mobile Cloud Data through Blind Storage',IEEE Transactions on Emerging Topics in Computing, vol. 3, No. 1, March 2015, pp. 127-138.

[10] Hui Lin , Li Xu, Yi Mu and Wei Wu, 'A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing', Future Generation Computer Systems, Elsevier, vol. 52, November 2015, pp. 125-136.