International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

A Light Weight Cryptographic Technique for Secure Outsourcing and Retrieval of Data in Cloud Computing

D Ramesh, B Rama

Abstract: ***Outsourcing large volumes of data to public cloud has the potential benefits to consumers. It also brings security issues as the cloud is treated as untrusted from the user point of view. Security issues may arise due to many reasons such as virtualization, resource pooling, elasticity, hidden hardware problems besides internal and external attacks launched by adversaries. Service Level Agreements (SLAs) between Cloud Service Provider (CSP) and cloud consumer are to be honoured for better social welfare. Therefore, it is indispensable to have mechanisms to ensure security to outsourced data when it is at rest and when it is in transit as well. Towards this end, many solutions came as found in the literature. However, most of the cryptographic methods employed were expensive. It is still an open challenge to develop light weight cryptographic methods for secure storage and retrieval or search for outsourced encrypted data. In this paper we proposed a methodology for light weight encryption which proved to be effective and suitable for cloud computing environments. An algorithm named Hybrid Lightweight Data Encryption (HLDE) is proposed and implemented. Empirical study is made on the same to validate our approach. The experimental results revealed that the proposed method is better than the state of the art in terms of high performance and strong security to outsourced data in cloud computing.***

Keywords: ***Cloud computing, security issues in cloud computing, data storage security, lightweight encryption, secure outsourcing***

I. INTRODUCTION

Cloud computing has brought a technological innovation in dealing with computing resources. Since it is an Internet based computing, it has changed the way Information Technology (IT) departments are working traditionally [31]. It paved way foroutsourcing large amount of data and computing tasks. Amazon EC2 (Elastic Compute Cloud), Google Cloud, Microsoft Azure and IBM cloud are some of the cloud platforms from different vendors. With cloud platforms in place, it became a common practice for enterprises to outsource data and computations to public cloud. In addition to this the outsourced data is subjected to search and search query integrity [4].

Manuscript published on 30 August 2019.
***Correspondence Author(s)
D. Ramesh, Assistant Professor in Computer Science, Department of Computer Science, University Campus College, Kakatiya
Dr. B.RAMA, Thirupathi, India in theyear of 2009. She is working as Assistant Professor in Computer Science at Department of Computer Science, University Campus College, Kakatiya

In the cloud computing platform performing keyword search on outsourced and encrypted data became an essential and important operation. There are research contributions on single keyword search and multi-keyword search as well. In [5] multi-keyword based fuzzy search is supported on encrypted outsourced data. In fact, such feature provides greater flexibility to end users when retrieving data based on the requirements.

In the literature many kinds of schemes are found on secure storage and retrieval of data in public cloud. Attribute based keyword search is explored in [4] where attributes are given importance in secure storage and retrieval of data. Multi-keyword fuzzy search with privacy preserving is implemented in [6] to have security, privacy and flexibility. A scheme is implemented for personalized search in [7] for improving efficiency in storage and retrieval of data. Efficient multi-keyword search with support for parallel processing is explored in [8]. Ranked keyword search for better results is investigated in [11], [12], [13] and [14]. There are many lightweight schemes proposed in [21], [22], [23], [26], [29], [30]and [33]. From the literature review it is understood that lightweight schemes could provide better performance in secure data storage and retrieval. However, lightweight encryption mechanism can be enhanced further in order to have better performance. This problem is addressed in this paper. Our contributions in this paper are as follows.

1. We proposed a lightweight encryption algorithm known as Hybrid Lightweight Data Encryption (HLDE) for improving performance in secure cloud storage and retrieval.
2. We built a prototype application to know the performance of the proposed algorithm with variety of workloads.
3. We evaluated the HLDE algorithm and compared its performance with the state of the art. The results showed that the HLDE outperformed the existing algorithms.

The remainder of the paper is structured as follows. Section 2 provides review of literature on various schemes used for secure storage and retrieval of data in cloud. Section 3 presents the proposed system in detail. Section 4 presents results of empirical study. Section 5 concludes the paper besides providing directions for future scope of the work.

II. RELATED WORK

This section reviews relevant literature on secure cloud storage and retrieval. The data outsourced to public cloud needs to be retrieved and searched for. Wang *et al.* [2] proposed a method for verifiable fuzzy keyword search over encrypted cloud data. The model is for better search performance and also provides secure communications among parties like data owners, users and cloud server. Fu *et al.* [1] proposed a multi-keyword ranked search on the data encrypted and outsourced. It also supports queries using synonyms thus providing better performance and effectiveness. However, semantics based search over encrypted data is not covered. Selvakumar *et al.* [16] employed data partitioning technique in order to have better solution for data security in public cloud. It has provision for misbehaving server localization and also error localisation. Fu *et al.* [17] proposed a method with semantic search capability besides privacy preserving approach. Conceptual graphs are used over encrypted data in order to achieve this and intended to enhance it further with NLP.

Conceptual graphs over encrypted data is used for semantic search as explored by Fu *et al.* [19]. Fu *et al.* [3] on the other hand proposed a method to have content aware search over cloud data. They employed a tree-based index structure in order to improve performance further. However, the sematic search over encrypted data is still a work to be done. Multi-keyword search over encrypted and outsourced data is explored in [5] but it lacks privacy preserving concept. In the same fashion, Khan *et al.* [18] proposed a ranked multi-keyword search with fuzzy logic enhancing user experience in search process. It could minimize overhead when compared to the state of the art. Wang *et al.* [6] proposed multi-keyword search that takes care of effective search and also privacy preserved. Security, accuracy and efficiency is thus achieved in searching phenomenon.

Wang *et al.* [11] proposed a ranked keyword search over outsourced and encrypted cloud data. They used a statistical measure known as relevance score with an indexing mechanism to improve search performance. Fu *et al.* [7] proposed a Personalized Ranked Search over Encrypted data (PRSE) with multi-keyword and privacy preserving support. It has search intentions to be carried out without disclosing private or sensitive information. Fu *et al.* [10] proposed multi-keyword ranked search with parallel processing capabilities in public cloud. They exploited tree based index for efficient processing. They defined security schemes with privacy requirements. However, they have not yet covered semantics-based search. Xia *et al.* [12] continued multi-keyword ranked search with an index structure to be part of Greedy depth first Search for achieving multi-keyword ranked search. However, they did not handle revocation of users and dishonest users. Wang *et al.* [8] proposed a privacy assured search mechanism for performing similarity search over encrypted outsourced data. It supports fuzzy search with privacy preserved. However, they have not focused on sequence of keywords and conjunction of keywords while searching. Li *et al.* [15] proposed an effective fuzzy keyword search that is used on cloud based encrypted outsourced data. They constructed fuzzy keyword sets in order to reduce complexity of the system. Li *et al.* [9] considered Personal Health Records (PHRs) for performing privacy key search on the outsourced data. They proposed a fine-grained authorization framework to achieve this. They ensured document privacy and query privacy.

As far as ranked keyword search is considered, Wang *et al.* [13] proposed a ranked search for improving usability of the system. They utilized Order Preserving Symmetric Encryption (OPSE) technique for the purpose of efficiency in searching and security guarantee. It does not have provision for multiple keywords though. Cao *et al.* [14], unlike [12], proposed multi-keyword ranked search with a privacy preserving technique. Strict privacy needs are considered and the notion of inner product similarity is used for effective implementation. The concept of attribute based encryption (ABE) is employed by Koo *et al.* [20],[32] and [34] for efficient data retrieval from public cloud with high level of security.

Baharan *et al.* [21] proposed a novel lightweight scheme for encryption of data in Mobile Cloud Computing (MCC). They employed Lightweight Homomorphic Encryption (LHE) for reduction of overhead in key generation and encryption mechanisms. Singh *et al.* [22] on the other hand explored advanced lightweight security schemes for IoT use cases. They studied lightweight block cipher, lightweight hash function, high performance systems and low resource devices. Liang *et al.* [23] proposed a hybrid encryption scheme with lightweight concepts. It is achieved by improving RSA algorithm followed by merger of AES and RSA for making a hybrid algorithm. Pitchai *et al.* [24] proposed a file sharing method base on searchable encrypted and outsourced data. It employs a keyword for every piece of data while performing encryption. Then it will make it easier for searching. Li *et al.* [25] proposed a scheme for lightweight search over encrypted data with phrases.

Tahir *et al.* [26] proposed used the concept of probabilistic trapdoor in order to have a lightweight security scheme that could improve performance in searching. However, query expressiveness is still a problem with the scheme. Secure medical image storage and retrieval over public cloud is studied by Vengadapurvaja *et al.* [27]. They used homomorphic encryption in order to have search over encrypted data. Bogdanov *et al.* [28] on the other hand proposed AES-based encryption method forsecure data storage and retrieval. Xu *et al.* [29] proposed a fully homomorphic encryption scheme based on Merkle tree in order to have secure and lightweight search over public cloud. It could reduce storage, computation and communication overhead. With respect to smartphone cloud, Zegers *et al.* [30] a cryptographic scheme which is lightweight and energy efficient. It provides security primitives for use authentication, encryption and decryption in the smart cloud environment. From the literature review, it is observed that the security schemes for cloud storage are lightweight. However, they need to be enhanced for better performance. In this paper the proposed scheme is more lightweight and provides performance improvement over the state of the art.

Retrieval Number: J10730881019/19©BEIESP
DOI: 10.35940/ijitee.J1073.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

III. PROPOSED SYSTEM

The proposed scheme is meant for reducing overhead and making the storage and retrieval process lightweight and effective. A Hybrid Lightweight Data Encryption (HLDE) algorithm is proposed based on different procedures such as key generation for generating security keys, secret sharing for application of visual secret sharing approach on textual data, transpose which is well known matrix operation and swap which is also widely used method to swap values. These four operations are combined together to form an algorithm for encryption and decryption. Table 1 shows the symbols used and their definitions in the proposed mechanism.

Symbol	Definition
A^T	Transpose matrix A
S_1, S_2	Two matrices with the size of (4×4)
K_1	Swap of k
ST_1, ST_2	Transpose matrices of S_1, S_2
$\otimes$	XNOR operation
A	Matrix
$E(\beta)$	Mean of β
$Final - S_1$, $Final - S_2$	final encrypted shares of the secret
$H(S)$	Entropy
K	Generate key
N	total number of elements obtained from the data
$P(S_i)$	Probability of S
S	Message
Secret 1, Secret 2	Shares of secret messages
T	transpose
B	values for which correlation needs to be calculated

Table 1: Symbols used

The key generation process is based on Diffie-Hellman algorithm which is widely used for key agreement. It will help any two parties communicating over network to have dynamic establishment of shared secret key automatically. In this paper Diffie-Hellman algorithm is modified in order to have 4x4 size matrix to be generated and exchanged instead of single key exchange as in conventional Diffie-Hellman algorithm. It also helps in generating private key for cloud and user randomly with the help of 4x4 size master random grid matrix. After key generation procedure, the secret sharing procedure is followed. The concept used in the visual secret sharing is employed to textual data in order to make it lightweight and effective. The method follows (2,2) access structure. XNOR operation is used in order to generate basic matrices. The secret sharing procedure is as follows.

1.Start
2.For each block of message
3. For each word of the block
4.For each bit in the word
5.If bit is zero Then
6.Choose any row randomly from C_0
7.Assign an element of the row to first share
8. Assign other element of the row to second share
Else if bit is one Then
9.Choose any row randomly from C_1
10. Assign an element of the row to first share
11. Assign other element of the row to second share
12. End If
13. End For
14. End For
15. End For
16. Convert shares to original form
17. End

Algorithm 1:Secret sharing algorithm

As shown in Algorithm 1, the steps are self-explanatory. There is difference between the big value is verified in the conditions and the procedure finally converts the two shares into the original form. After this, the transport procedure is follows. The input matrix is converted in such a way that rows become columns and columns become rows. It is shown as in Eq. 1.

$$\text{Output} = (\text{input})^T \quad (1)$$

The input matrix is denoted as input while the output matrix is denoted as output. After this, swap procedure is applied. With respect to swap procedure, all upper triangle entries of matrix are swapped with lower triangular entries. It is mathematically shown as in Eq. 2.

$$\forall aij \in A : Swap(aij, aij); i \neq j, i, j = 1, \ldots n. \quad (2)$$

After performing swapping encryption and decryption procedures are followed. The proposed encryption is known as Hybrid Lightweight Data Encryption (HLDE). The algorithm is as follows.

Algorithm:Hybrid Lightweight Data Encryption (HLDE)

1. **Start**
2. **Divide secret message into number of 16 bytes blocks (4x4 matrix)**
3. **Pass each block to secret sharing procedure to generate two shares**
4. **Use key generation procedure and use XNOR on K (secret key) and two shares**

$$S_1 = K \otimes \text{Secret } 1$$
$$S_2 = K \otimes \text{Secret } 2 \quad (3)$$

5. **Apply transport on two S1 and S2**

$$ST_1 = Transpose\ (S1)$$
$$ST_2 = Transpose\ (S2) \quad (4)$$

6. **Apply swap procedure**

$$K_1 = Swap(k) \quad (5)$$

7. **Generate encrypted shares**

$$Final - S_1 = ST_1 \otimes K_1$$
$$Final - S_2 = ST_2 \otimes K_1 \quad (6)$$

8. **Repeat the steps from 2 to 6 for encrypting complete secret message**
9. **Transfer final shares to destination**
10. **End**

Algorithm 2: Hybrid lightweight data encryption algorithm

As presented in Algorithm 2, encryption procedure is carried out. The procedure ends with generation of encrypted shares that can be transmitted to destination.

Then the decryption procedure is just opposite to the encryption procedure. In other words, the reverse procedure needs to be followed for the decryption process. Figure 1 shows a flow chart visualizing the encryption procedure.

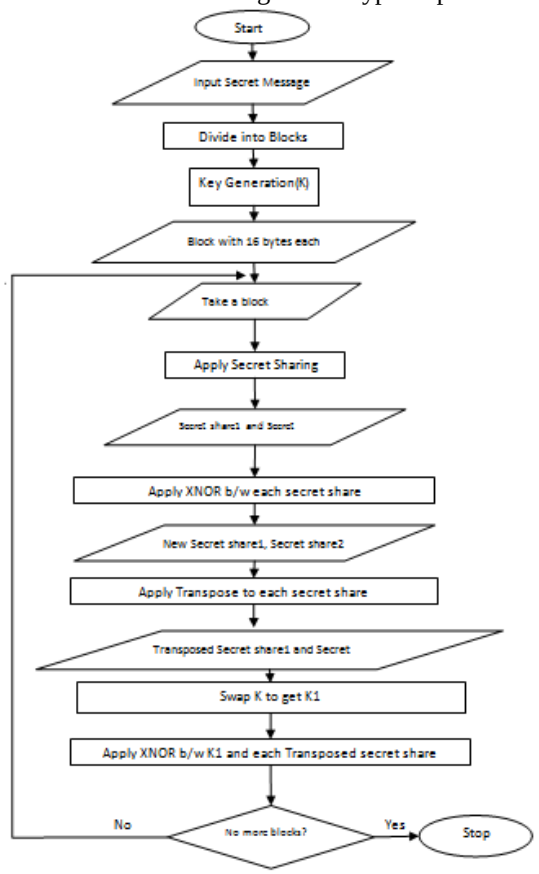

Figure 1:Flow chart of the proposed hybrid lightweight data encryption algorithm

As presented in Figure 1, The encryption flow is visualized to understand it with ease. It has different phases like taking input secret message that needs to be encrypted. The message is divided into different number of blocks. Then key generation procedure is followed. Afterwards, an iterative process is followed which comprises of the steps as described here. One block is taken from message, secret sharing is applied, XNOR operation is applied on each secret share, transpose procedure is applied, then swap is applied finally XNOR is employed to complete the encryption procedure for given block. This way all blocks are subjected to encryption.

IV. EXPERIMENTAL RESULTS AND EVALUATION

Experiments are made with different workloads using the proposed HLDE algorithm. Its performance is compared with many state of the art algorithms known as DES, AES and IDEA. These are all cryptographic algorithms that are widely used. The performance of the proposed method (HLDE) is compared with existing algorithms in terms of original text, encrypted data and decrypted data. Obviously the original text and decrypted data are same while the encrypted data is shown based on the procedure followed by each algorithm.

Cryptography technique	Original secret	Encrypted data	Decrypted data
DES	ABCDEFABCDEFABCD	++ sC|r Ã P^ « ?{A	ABCDEFABCDEFABCD
AES	ABCDEFABCDEFABCD	÷üjðK?hTMØ	ABCDEFABCDEFABCD
IDEA	ABCDEFABCDEFABCD	Ôî+±0 m{WyQ%	ABCDEFABCDEFABCD
HLDE	ABCDEFABCDEFABCD	´Eå ª!UJ,7] ~ Õ¡È	ABCDEFABCDEFABCD

Table 2: Encrypted and decrypted data samples for different algorithms

As shown in Table 2, encrypted data and decrypted data of the DES, AES, IDEA and the proposed algorithm are presented.

Cryptography technique	Key size	Key space
DES	64	264
AES	128	2128
IDEA	128	2128
HLDE	128	2128

Table 3: Encryption schemes and their key size and key space

Table 2 shows the cryptography techniques and their corresponding key size and key space. The key size of DES is 64, AES, IDEA and proposed 128. Based on the key size corresponding key space is used.

Correlation Analysis	
AES	-0.35
DES	0.28
IDEA	-0.02
PROPOSED	0.35

Table 4: Shows correlation analysis

The correlation analysis shows the algorithms and their corresponding correlation value. The correlation is computed between original data and encrypted data. Ideally zero correlation shows better performance.

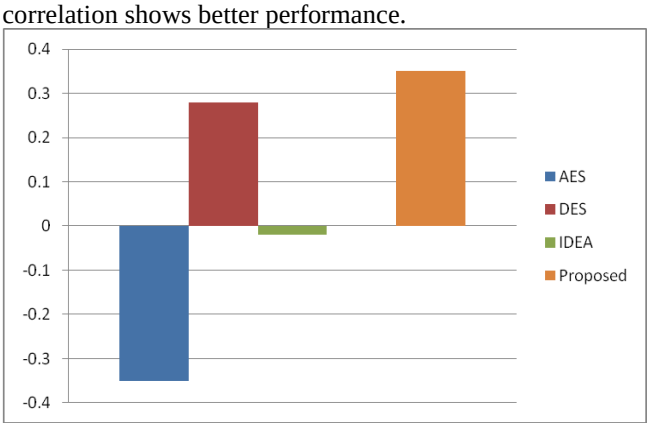

Figure 2: Shows result of correlation analysis

As presented in Figure 2, it is understood that correlation value is in negative for AES and IDEA algorithms. For DES it is 0.28 and proposed method it is 0.35. The zero value generally reveals good performance.

Retrieval Number: J10730881019/19©BEIESP
DOI: 10.35940/ijitee.J1073.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Entropy	
AES	3.8
DES	2.8
IDEA	4
PROPOSED	6.4

Table 5: Entropy analysis

As presented in Table 5, the entropy value of each algorithm is observed. Entropy measures randomness.

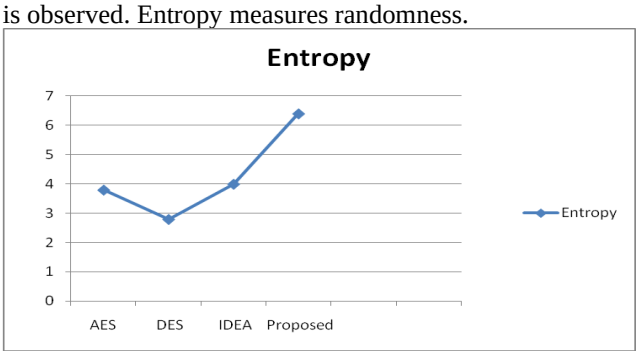

Figure 3: Shows entropy performance comparison

As presented in Figure 3, it is clear that the entropy of the proposed method is high. It indicates that the randomness probability is high which reveals better performance in the proposed secure storage and retrieval of data in public cloud.

File Size (KB)	Execution Time for Encryption (milliseconds)			
	DES	AES	IDEA	PROPOSED
40	50	30	80	28
227	80	50	150	35
487	100	80	250	45
5478	500	400	1000	280
15276	1500	1400	1700	1050

Table 6: Shows execution time for encryption against different workloads

As shown in Table 6, the execution time for encryption in case of algorithms like DES, AES, IDEA and the proposed is presented against workloads like 40 KB to 15276 KB with different increments.

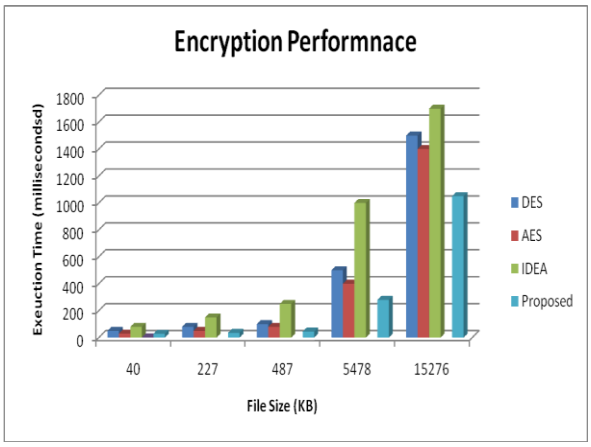

Figure 4: Shows execution time of algorithms for encryption against different workloads

As presented in Figure 4, it is observed that the workload is considered in horizontal axis while the vertical axis shows execution time in milliseconds. The file size has its impact on the execution time. At the same time, the performance of the proposed method is higher than that of other methods. In other words, it needs less time to perform encryption. The rationale behind this is that the proposed method is lightweight.

File Size (KB)	Execution Time for Decryption (milliseconds)			
	DES	AES	IDEA	PROPOSED
40	30	20	30	18
227	50	40	40	35
487	150	80	80	75
5478	800	450	800	400
15276	1750	1500	1700	1450

Table 7: Shows execution time for decryption against different workloads

As shown in Table 7, the execution time for decryption in case of algorithms like DES, AES, IDEA and the proposed is presented against workloads like 40 KB to 15276 KB with different increments.

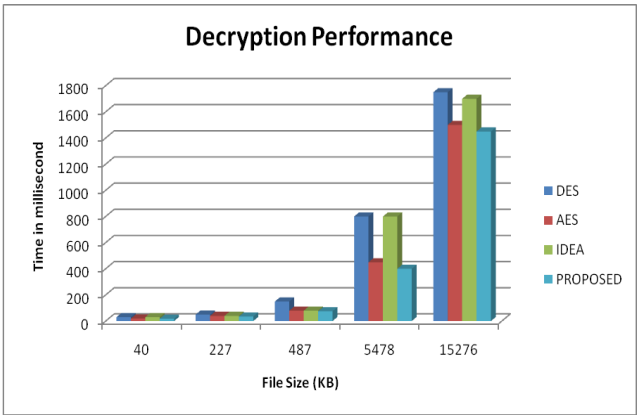

Figure 5: Shows execution time of algorithms for decryption against different workloads

As presented in Figure 4, it is observed that the workload is considered in horizontal axis while the vertical axis shows execution time for decryption of given workload in milliseconds. The file size has its impact on the execution time. At the same time, the performance of the proposed method is higher than that of other methods. In other words, it needs less time to perform decryption. The rationale behind this is that the proposed method is lightweight.

V. CONCLUSION AND FUTURE WORK

In this paper a lightweight encryption and decryption schemes are proposed by applying the traditional visual secret sharing method to textual data. It is a hybrid approach with lightweight mechanism for better performance. The hybrid approach includes operations such as generation of security keys, the procedure related to secret sharing, transpose of matrices, and swapping of matrices. The proposed methodology includes both confusion and diffusion to make it highly secure. The former is to change data drastically while the latter is to reflect in many characters of output when a single character is modified in the input.

Retrieval Number: J10730881019/19©BEIESP
DOI: 10.35940/ijitee.J1073.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

These two are realized with the help of procedures namely transpose and swap. The proposed encryption algorithm is known as Hybrid Lightweight Data Encryption (HLDE). It is evaluated in terms of correlation, entropy, execution time for encryption and decryption. The performance of the HLDE is compared with state of the art security schemes like DES, AES and IDEA. The empirical results revealed that the proposed method for encryption and decryption is lightweight and works faster than the existing schemes. This kind of scheme is useful for storing and retrieving of data in cloud in a secure fashion. In future, we investigate on the performance of the proposed algorithm for data dynamics on outsourced encrypted data. Another direction for future work is to find suitability of the proposed algorithm for Internet of Things (IoT) based applications that outsource data to public cloud.

REFERENCES

1. Fu, Z., Sun, X., Linge, N., & Zhou, L. (2014). Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query. IEEE Transactions on Consumer Electronics, 60(1), 164–172.
2. Wang, J., Ma, H., Tang, Q., Li, J., Zhu, H., Ma, S., & Chen, X. (2013). Efficient verifiable fuzzy keyword search over encrypted data in cloud computing. Computer Science and Information Systems, 10(2), 667–684.
3. Fu, Z., Sun, X., Ji, S., & Xie, G. (2016). Towards efficient content-aware search over encrypted outsourced data in cloud. IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications. P1-9.
4. Zheng, Q., Xu, S., & Ateniese, G. (2014). VABKS: Verifiable attribute-based keyword search over outsourced encrypted data. IEEE INFOCOM 2014 - IEEE Conference on Computer Communications. P1-9.
5. Fu, Z., Wu, X., Guan, C., Sun, X., & Ren, K. (2016). Toward Efficient Multi-Keyword Fuzzy Search Over Encrypted Outsourced Data with Accuracy Improvement. IEEE Transactions on Information Forensics and Security, 11(12), 2706–2716.
6. Wang, B., Yu, S., Lou, W., & Hou, Y. T. (2014). Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. IEEE INFOCOM 2014 - IEEE Conference on Computer Communications.
7. Fu, Z., Ren, K., Shu, J., Sun, X., & Huang, F. (2016). Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement. IEEE Transactions on Parallel and Distributed Systems, 27(9), 2546–2559.
8. Wang, C., Ren, K., Shucheng Yu, & Urs, K. M. R. (2012). Achieving usable and privacy-assured similarity search over outsourced cloud data. 2012 Proceedings IEEE INFOCOM. P1-9.
9. Ming Li, Shucheng Yu, Ning Cao and Wenjing Lou. (2010). Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing, p1-12.
10. FU, Z., SUN, X., LIU, Q., ZHOU, L., & SHU, J. (2015). Achieving Efficient Cloud Search Services: Multi-Keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing. IEICE Transactions on Communications, E98.B(1), 190–200.
11. Wang, C., Cao, N., Ren, K., & Lou, W. (2012). Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data. IEEE Transactions on Parallel and Distributed Systems, 23(8), 1467–1479.
12. Xia, Z., Wang, X., Sun, X., & Wang, Q. (2016). A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data. IEEE Transactions on Parallel and Distributed Systems, 27(2), 340–352.
13. Wang, C., Cao, N., Li, J., Ren, K., & Lou, W. (2010). Secure Ranked Keyword Search over Encrypted Cloud Data. 2010 IEEE 30th International Conference on Distributed Computing Systems. P1-10.
14. Cao, N., Wang, C., Li, M., Ren, K., & Lou, W. (2014). Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data. IEEE Transactions on Parallel and Distributed Systems, 25(1), 222–233.
15. Li, J., Wang, Q., Wang, C., Cao, N., Ren, K., & Lou, W. (2010). Fuzzy Keyword Search over Encrypted Data in Cloud Computing. 2010 Proceedings IEEE INFOCOM. P1-5.
16. Selvakumar, C., Rathanam, G. J., & Sumalatha, M. R. (2013). PDDS - Improving cloud data storage security using data partitioning technique. 2013 3rd IEEE International Advance Computing Conference (IACC). P1-5.
17. Fu, Z., Huang, F., Ren, K., Weng, J., & Wang, C. (2017). Privacy-Preserving Smart Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data. IEEE Transactions on Information Forensics and Security, 12(8), 1874–1884.
18. Khan, N. S., Krishna, C. R., & Khurana, A. (2014). Secure ranked fuzzy multi-keyword search over outsourced encrypted cloud data. 2014 International Conference on Computer and Communication Technology (ICCCT). P1-9.
19. Fu, Z., Huang, F., Sun, X., Vasilakos, A., & Yang, C.-N. (2016). Enabling Semantic Search based on Conceptual Graphs over Encrypted Outsourced Data. IEEE Transactions on Services Computing, 1–1.
20. Koo, D., Hur, J., & Yoon, H. (2013). Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage. Computers & Electrical Engineering, 39(1), 34–46
21. Mohd Rizuan Baharon, Qi Shi and David Llewellyn-Jones. (2015). A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing. IEEE, p1-9.
22. Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing. P1-18.
23. Changing Liang, Ning Ye, Malekian, R., & Ruchuan Wang. (2016). The hybrid encryption algorithm of lightweight data in cloud storage. 2016 2nd International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR). P1-7.
24. Pitchai, R., Jayashri, S., & Raja, J. (2016). Searchable Encrypted Data File Sharing Method Using Public Cloud Service for Secure Storage in Cloud Computing. Wireless Personal Communications, 90(2), 947–960.
25. Li, M., Jia, W., Guo, C., Sun, W., & Tan, X. (2015). LPSSE: Lightweight Phrase Search with Symmetric Searchable Encryption in Cloud Storage. 2015 12th International Conference on Information Technology - New Generations. P1-5.
26. Tahir, S., Ruj, S., Rahulamathavan, Y., Rajarajan, M., & Glackin, C. (2017). A New Secure and Lightweight Searchable Encryption Scheme over Encrypted Cloud Data. IEEE Transactions on Emerging Topics in Computing, 1–14.
27. Vengadapurvaja, A. M., Nisha, G., Aarthy, R., & Sasikaladevi, N. (2017). An Efficient Homomorphic Medical Image Encryption Algorithm for Cloud Storage Security. Procedia Computer Science, 115, 643–650.
28. Bogdanov, A., Mendel, F., Regazzoni, F., Rijmen, V., & Tischhauser, E. (2014). ALE: AES-Based Lightweight Authenticated Encryption. Lecture Notes in Computer Science, 447–466.
29. Xu, J., Wei, L., Zhang, Y., Wang, A., Zhou, F., & Gao, C. (2018). Dynamic Fully Homomorphic encryption-based Merkle Tree for lightweight streaming authenticated data structures. Journal of Network and Computer Applications, 107, 113–124.
30. Zegers, W., Chang, S.-Y., Park, Y., & Gao, J. (2015). A Lightweight Encryption and Secure Protocol for Smartphone Cloud. 2015 IEEE Symposium on Service-Oriented System Engineering. P1-10.
31. Venkateshwarlu Velde, B. Rama (2018),A Framework for User Priority Guidance based Scheduling for Load Balancing in Cloud Computing, published in International Journal of Systems, Science and Technology, 2018, pp. 1473-8031.
32. Vurukonda, N., & Thirumala Rao, B. (2019). DC-MAABE: Data Centric Multi-Authority Attribute Based Encryption on Cloud Storage. Journal of Computational and Theoretical Nanoscience, 16(5-6), 1893-1901.
33. Venkatakotireddy, G., Rao, B. T., & Vurukonda, N. (2018). A Review on Security Issue in Security Model of Cloud Computing Environment. In Artificial Intelligence and Evolutionary Computations in Engineering Systems (pp. 207-212). Springer, Singapore.
34. Rao, B. T. (2016). A study on data storage security issues in cloud computing. Procedia Computer Science, 92, 128-135.
35. Naveen Kumar, R., Vege, H.K. & Sreeram, G. 2019, "Patient treatment interval used in forecast algorithm and solicitations in hospital queuing management", International Journal of Innovative Technology and Exploring Engineering, ISSN:2278-3075, vol. 8, no. 7, pp. 3003-3007.
36. Reddy, L.H., Thamognudu, Y. & Sreeram, G. 2019, "Deployment of a secured web application using cryptanalysis in cloud environment", International Journal of Engineering and Advanced Technology, ISSN:2249-8958, vol. 8, no. 4, pp. 1841-1844.

37. Sreeram, G., Kanumuri, M.K. & Bodduluri, M. 2019, "Improving cloud data storage performance based on calculating score using data transfer rate between the internetwork drives", International Journal of Engineering and Advanced Technology, ISSN:2249-8958, vol. 8, no. 4, pp. 1830-1835.
38. Naveen Kumar, R., Vege, H.K. & Sreeram, G. 2019, " A Perspective of Probabilistic Misbehavior Detection Scheme in Vehicular Ad-hoc Networks", International Journal of Innovative Technology and Exploring Engineering,ISSN:2278-3075, vol. 8, no. 6, pp.1098-1102.

AUTHORS PROFILE

D. Ramesh completed M.Tech(Computer Science) From School of IT,JNTU Hyderabad and pursuing PhD in the department of Computer Science, Kakatiya University, Warangal. Present working as Assistant Professor in Computer Science, Department of Computer Science, University Campus College, KakatiyaUniversitysince ten years. Area of interest is Cloud Computing, cryptography Network Security. Published papers in IEEE InternationalConferences and International Journals.

Dr. B.RAMA received her Ph.D. Degree in Computer Science from PadmavatiMahila Visvavidyalayam, Thirupathi, India in theyear of 2009. She is working as Assistant Professor in Computer Science at Department of Computer Science, University Campus College, KakatiyaUniversitysince ten years. Her area of interest is Artificial Intelligenceand Data Mining.She is the author or co-author of various scientific, technical papers mainly in IEEE, Springer InternationalConferences and International Journals.