International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

# Two Pass Multidimensional Key Generation and Encryption Algorithm for Data Storage Security in Cloud Computing

**Mohd. Tajammul, Rafat Parveen**

***Abstract*: Many companies which essentially required cloud computing services are still in ambivalence whether to adopt it or not. In this research paper an attention has been drawn on security of storage as a Service which is an integral part of Infrastructure as a Service which provide famous CSP, AWS. Whenever someone rent the storage from the cloud service provider, chances of its compromising can take place. Therefore it is intelligence to encrypt the data before uploading it to the cloud and more intelligently divide the data into fragments and encrypt these fragments separately and then upload on cloud. Suppose that if this data is divided into n fragments then n algorithm are required to encrypt these fragments or use single one algorithm and change its key n times otherwise if only one key will be used and someone steal this key then all fragments will be decrypted with the same key. Many algorithms like DES, AES, RSA, Elgamal and Blow Fish are there but they all are static in nature and one more weakness of these algorithms is that size of encrypted file increased. While some researchers used these algorithms in combination and some used double encryption, nevertheless nature remains static and decrypted file size increase rapidly. Now, there is a requirement to design a data sensitive algorithm which could sense data and produce different key for different data automatically. In this paper Two Pass Multidimensional Key Generation and Encryption Algorithm has been proposed which will sort the above problem. Another beauty of this algorithm is that it checks the integrity of the documents while decrypting. Out of millions or billions of characters if only one character or word is altered or removed then this algorithm will show that documents integrity has been violated.***

***Index Terms*: Cloud Computing; Two Pass Algorithm; Data Sensitive; Storage Security; User Independent.**

## I. INTRODUCTION

Cloud Computing is a technology for performing computation through Internet on remote location. Cloud computing was first coined by Prof. John McCarthy in 1960. Initially cloud computing was growing rapidly and its field was spreading fast. Large scale companies were adopting the cloud computing happily. As soon as the news of data leakage and hacking from cloud came, it leveraged a bad impact in users' mind.

**Revised Manuscript Received on 30 July 2019.**
***** Correspondence Author
**Mohd. Tajammul***, Department of Computer Science, Jamia Millia Islamia, New Delhi, India.
**Rafat Parveen**, Department of Computer Science, Jamia Millia Islamia, New Delhi, India.



Cloud Computing is a very popular and versatile environment to support commercial business industries. It is rich with a no. of definitions. According to Prof. John McCarthy

"If computers of the kind I have advocated become the computers of the future, computing may someday be organized as a public utility just as the telephone system is a public utility. The computer utility could become the basis of a new and important industry"[7].The National Institute of Standards and Technology (NIST) define cloud computing as "A model for enabling convenient, on demand network access to a shared pool of congurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models" [18, 21].

### A. Deployment models of cloud computing

- **Public cloud-:** This is one of the types of cloud deployment model in which everybody is allowed to avail services. It is highly suggested to go for this cloud model if data or computation is not highly sensitive or secure [7].
- **Private cloud-:** This is one of the types of cloud deployment model in which everybody is not allowed to avail services. It is highly suggested to go for this cloud model if data or computation is highly sensitive or secure. It is available for any particular company, organization or an individual [19, 23].
- **Community cloud-:** This is one of the types of cloud deployment model in which every body from a community or from a particular group only is allowed to avail services. It is highly suggested to go for this cloud model if data or computation is of middle level sensitive or secure [19, 22].
- **Hybrid cloud-:** This is one of the types of cloud deployment model in which everybody is allowed to avail services. It is combination of any of the above two cloud models [7, 22, 23].

### B. Service Models of cloud computing

- **Software as a Service (SaaS)-:** Under this service, software is provided to the client on which he or she can perform operations for instance Gmail. Some well known SaaS providers are SalesForce.com, Microsoft, IBM and Oracle, NetSuite [18].
- **Platform as a Service (PaaS)-:** Under this service, a platform is given to the client, on which client can develop his or her applications. Some well known PaaS providers are Microsoft Azure, GAE [18].

- **Infrastructure as a Service (IaaS)-:** An infrastructure like CPU or storage is given to the client, on which he or she can perform computation or upload data for future use. Popular IaaS providers are Amazon Web Services Joyent, Flexiscale, GoGrid [18].

### C. Issues of Security in cloud computing [21]

- Issues of security at SaaS level
- Issues of security at PaaS level
- Issues of security at IaaS level

Storage as a Service is an integral part of Infrastructure as a Service; hence this research paper focuses on security at I-a-a-S level.

### D. Our Contribution

In this work, we have studied that how to develop an algorithm based on matrices rather than group. We have proposed algorithms which will sense the input data automatically and will produce the encryption key in the form of matrix. Our main motto is to use multidimensional key rather than single dimensional. This is first attempt to go towards the matrix approach and multidimensional key. We have proposed three algorithms that is encryption algorithm, decryption algorithm and integrity testing algorithm. We have summarized our contribution as under:

- **Firstly,** we have designed an encryption algorithm which will sense the data automatically and will then produce the encryption key which will be used for encryption and finally it will be stored at local sever after applying steganography.
- **Secondly,** we have designed decryption algorithm corresponding to our encryption algorithm which will decrypt the encrypted data after taking key from local server.
- **Thirdly,** we have designed integrity testing algorithm which will test the integrity of the input data and if any of the character is altered, corresponding entry of Integrity matrix I will be differ from the entry of Frequency matrix F.
- **Fourthly,** we have proposed architecture to support our whole idea which will show the flow of execution of all the above algorithms.

**Organization** of the paper is as Section-2 discusses Literature Review, Section-3 discusses Research Gap, Section-4 discusses Problem Formulation, Section-5 discusses Overview of Algorithm, and Section-6 discusses implementation and validation and finally Section-7 Conclude the paper with future research directions.

## II. LITERATURE REVIEW

In [1], Liefi Wei et al. Proposed SecCloud and SecHDFS for storage and computation which encrypt the data before sending it to the cloud and before computation data will be decrypted without intervention of service provider. In [2], Zuojie et al. propose a scheme for multitenant environment to search with authorized keyword. Which solves the problem of finding encrypted files on storage in cloud computing. In [3], Hassan Rashed, proposed infrastructure and data auditing in cloud computing where author has divided security auditing issues into two categories that is data auditing and infrastructure auditing.

In [4], Laurace T. Yang et al. Proposed GNFS algorithm with parallel block and also Weidman algorithm for RSA security in cloud computing. Authors have also discussed the limitations of RSA and also discussed how GNFS is used in factoring large integer having more than 101 digits. In [5], Den Bonch and Mathew Franklin proposed an identity based encryption from Weil paring where authors shown a model based on bilinear map between groups and also given several applications of such system. In [6], Ali Azougaghe et al. proposed an efficient algorithm for data security in cloud computing where they encrypted data by AES and encrypted key produced by AES, by Elgamal. Then they sent data on cloud and stored key at local server.

In [7], Mohd. Tajammul, Rafat Parveen and Mohd. Shahnawaz discussed a no. of security issues at various models as well as a no. of solutions to overcome those issues. In [8], Subhashini and V. Kavitha discussed a survey on security issues on service models of cloud computing where authors discussed 14 security issues on SaaS and some on issues on PaaS some rest on Iaas. A large no. of solutions and tests has also been suggested to overcome these issues. In [9], Dimitrias Zissis, Dimitrias Lekkas addressed cloud security issues in tabular form representation by dis- cussing levels of security users and security requirements and threats also.

In [10], Manas MN et al. discussed cloud computing issues and methods to overcome. Authors have discussed there isolation on the basis of SaaS, PaaS and IaaS and finally isolation at VM in memory and cache in multitenant environment. In [11], Micheal Armbrust, shows a view of cloud computing where they proposed to clear the cloud away from the true potential and obstacle posed by cloud computing capabilities. In [12], Manish M Potey et al. proposed a homomorphic encryption for security of cloud data. Authors showed that computation is performed on encrypted data in public cloud and results will be saved on users system. In [13], P. Ravi Kumar et al. discussed various data security issues as well as resolution technique in cloud computing.

In [14], Hsun Chuhang et al. proposed an efficient privacy protection technique for cloud computing which satisfy the users' requirements of privacy and also maintain performance of the system at the same time. In [15], Qian wang et al. Tried to enable public auditability as well as data Two Passs for cloud storage. Authors discussed integrity, public auditability and dynamic data operations. In [16], Mahindha proposed a double encryption by applying DES algorithm on plain data and again applied RSA on encrypted data produced by DES and hence achieved two level encryption. In [18], Mohd Tajammul and Rafat Parveen, discussed big ten information security management system standards and their effect on cloud computing.

In [19], Mohd Tajammul and Rafat Parveen, discussed big ten information security management system standards. In [20], Tim Mather, Subra Kumaraswamy discussed infrastructure security, security of data and storage, security management in cloud and also identity access and management as well as key exchange and problem associated with it.

## III. MOTIVATION AND RESEARCH GAP

Encryption-Decryption plays very important role in the field of security. Literature review reveals that starting from DES, AES and RSA, a lot of algorithm and framework have been proposed for data storage security in cloud computing but all of them are of static nature, those takes key from user and don't sense data more over all of them are taking key only in single dimension. Hence there is deficiency of an algorithm in this field which is Two Pass in nature and data dependent rather user dependent so that mentioned deficiency could be eliminated and the gap can be fulfilled.

## IV. PROBLEM FORMULATION

Under this section, a system framework has been discussed and in next two sections a brief overview of proposed algorithm and design goals have been discussed.

### A. Working framework

As shown in Fig.1, original file will be divided into multiple files and then two Pass algorithm will be applied on each sub file separately which will generate encryption key in the form of matrix and also produce encrypted files.

All these encrypted files will be uploaded on to cloud storage at different-different location and the key will be stored at local server after applying stenography. By storing these files at different-different locations decrease the probability of stealing and leakage of whole data at once.

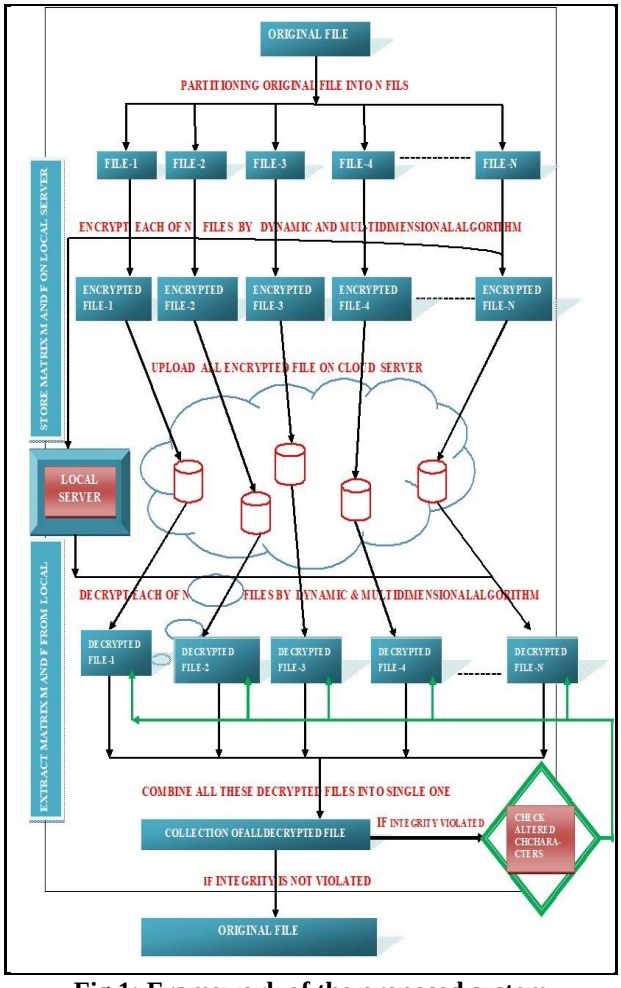


**Fig.1: Framework of the proposed system**

For decryption purpose, encrypted files will be downloaded from the cloud storage and keys will be extracted from local server and then Two Pass Algorithm for decryption will be applied to decrypt all sub files and then all decrypted sub files will be combined to produce single file. This file will be tested against integrity. If integrity is violated, testing will be done

## V. BRIEF OVERVIEW OF ALGORITHM

**Encryption -** It will take each sub file and will generate key separately and encrypt data, upload it at cloud storage and store key at local server.

**Decryption -** Download data from cloud storage and extract key from local server decrypt data and produce original file.

**Integrity Testing -** If integrity is violated then all sub files will be tested and checked which one has been modified and efforts will be applied to rectify.

### A. Design goals

The proposed algorithm has been designed to achieve following objectives.

- Storage security.
- To decrease the probability of stealing or leakage of whole data at once.
- To make cloud storage more versatile and to remove the fear of hacking.

### B. Proposed Algorithm

Proposed algorithm is based on generating the matrices of same order based on sensing the data input. In the proposed algorithm five matrices named F as frequency matrix, R as reduced matrix, C as character matrix, S as symbol matrix and finally M as unique matrix which contains unique entries mixture of symbols and characters will be produced. This M will work as key for encryption. Each matrix has its unique contribution in data sensing, Two Pass Key Generation, encryption, decryption and integrity testing.

### C. Merits of Proposed Algorithm

- It generates key in first Pass. If document is different, key is different.
- It generate multidimensional key in the form of matrix.
- Each of five matrices has unique contribution.
- Out of five matrices we need to store only two matrices at local server.
- Size of plain text and encrypted text remain same and not increased as it increased drastically in the case of DES, RSA and various other algorithms. Refer Table 3.
- Size of the encrypted and decrypted file remains same which eliminate one of the drawbacks of DES.
- This algorithm is more secure because it works in two Pass same as code produced by two pass compiler is more powerful in comparison to the one pass compiler. In first Pass it generates the key and produce cipher text and in second pass it perform decryption to generate plain text from cipher text.
- It is very easy to understand because it is based on ASCII values of characters and also on their respective positions.

- Reliable because it is working well with more data than shown in the given tables under implementation.

**Algorithm 1:** Encryption Pass

**Input:** *φ as Plain Text*
**Output:** *ψ as Cipher Text and Key*

```
1 i ←0, j ←0
2 F ←char Freq (φ)// Computer Char Frequencies
3 p ←randomPrime  29 ≤ p ≤ 97// Generate Prime
4 R ←F%p  // Take Modular Division
5 C ←char (R + ASCII (a − z, 0 − 9))
6 S ←ASCII (S) >ASCII (R)
7 while i < 6 do
8     while j < 6 do
9         if (C has duplicate entries) then
10            C_DE ←S_CE
11            M ←C
12        else
13            M ←C
14        end
15        + + j
16    end
17    + + i
18 end
19 Key ←M
20 ψ ←char_a(φ) ←Key[0][0]
21 ψ ←char_b(φ) ←Key[0][1]
22 ψ ←char_c(φ) ←Key[0][2]
23 .....
24 .....
25 ψ ←char_z(φ) ←Key[4][1]
26 ψ ←char_0(φ) ←Key[4][2]
27 ψ ←char_1(φ) ←Key[4][3]
28 .....
29 .....
30 ψ ←char_9(φ) ←Key[5][5]
31 Upload ψ on Cloud Server
32 Store Key and matrix F on Local Server
33 End
```

**Note-:** DE→ Duplicate Entries, CE→ Corresponding Entries

**Algorithm 1:** Decryption Pass

**Input:** ψ as Cipher Text and Key

**Output:** φ as Plain Text

```
1  read ψ char by char //Read Encrypted file
2  i ←0, j ←ψ.length // Initiate I by 0 and J By File Length
3  Match and replace ψ[i] with Key by following 4 to 35
steps
4  while i < j do
5      if ψ[i] == Key[0][0] then
6          ψ[i] ←a
7      end
8      if ψ[i] == Key[0][1] then
9          ψ[i] ←b
10     end
11     if ψ[i] == Key[0][2] then
12         ψ[i] ←c
13     end
14     .....
15     .....
16     if ψ[i] == Key[4][1] then
17         ψ[i] ←z
18     end
19     if ψ[i] == Key[4][2] then
20         ψ[i] ←0
21     end
22     if ψ[i] == Key[4][3] then
23         ψ[i] ←1
24     end
25     if ψ[i] == Key[4][4] then
26         ψ[i] ←2
27     end
28     .....
29     .....
30     if ψ[i] == Key[5][4] then
31         ψ[i] ←8
32     else
33         ψ[i] ←9
34     end
35 + + i
36 End
```

**Algorithm 2:** Integrity Testing

**Input:** $\psi_d$ as Decrypted Text

**Output:** Integrity Testing

```
1  Extract matrix F from Local Server// Computed by Algorithm 1
2  I ← charFreq(ψd)
3  Test equality between I and F by following steps
4  while i < 6 do
5      while j < 6 do
6          if F[i][ j] == I[i][ j] then
7              Integrity is preserved
8          else
9              Integrity is not preserved
10         end
11         + + j
12     end
13     + + i
14 End
```

## VI. IMPLEMENTATION AND VALIDATION

To evaluate performance of our algorithm (Two Pass Algorithm) we have designed application in java version jdk1.6.0 and NetBeans IDE7.2.1 on Intel Core i3-5005U CPU @ 2.00GHz, 8GB RAM, 1TB HDD, 64 bit Windows Pro Operating System. All the experiments have been done on single threaded machine. All the experiments have been performed 10 times at least. First of all we have shown experiment of our algorithm and then we have performed experiment on standard algorithm that is DES on same environment and then Efficient Algorithm [6] for comparison purpose. Parameters for comparison are as:

- Time Vs File-size
- Encrypted File-size

### A. Uploading Time Computation

To compute uploading time we have taken files of 50KB, 100KB, 200KB, 500KB, 1000KB and 2000KB and applied encryption function of our algorithm to encrypt this data and produce encrypted file to be uploaded on cloud storage and send produced key to local server after applying stenography. We have computed same function by using DES and Efficient algorithm in same environment that is on jdk1.6.0 and NetBeans7.2.1 on same system. Table 1, shows the results and Graph 1, shows comparison among time encryption time of these three algorithms.

### B. Downloading Time Computation

To compute downloading time we have taken encrypted files of 50KB, 100KB, 200KB, 500KB, 1000KB and 2000KB which were encrypted by Two Pass algorithm and uploaded on cloud storage and extracted key from local server applied decryption function of our algorithm to decrypt this data and produce plain file and after that we applied integrity testing function of our algorithm if integrity is maintain then store this file as original file otherwise check which of the character and consequently words have been changed or modified and try to rectify them. Then we have run DES algorithm and Efficient Algorithm for same data on same environment on same system for comparison purpose and stored the results in Table 2, and eventually sketched a comparison graph which is shown in Graph2.

**Table 1: Uploading Time Computation**

| File Size(KBs) | Two Pass Algorithm | DES Algorithm | Efficient Algorithm[6] |
|---|---|---|---|
| **50KB** | 0 | 1 | 2 |
| **100KB** | 1 | 2 | 2 |
| **200KB** | 1 | 3 | 3 |
| **500KB** | 2 | 7 | 3 |
| **1000KB** | 4 | 13 | 6 |
| **2000KB** | 7 | 25 | 11 |

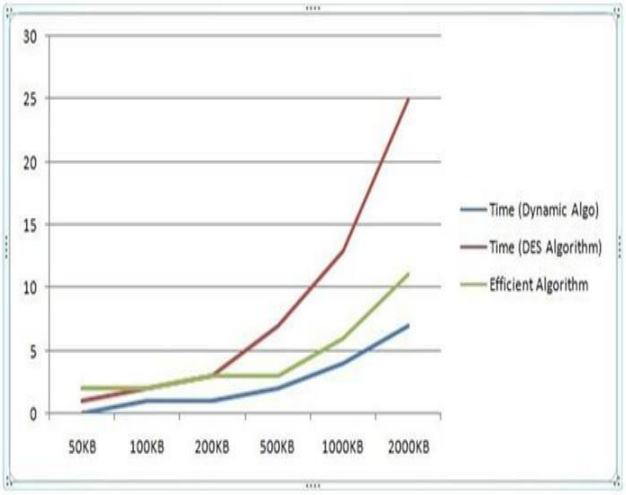


**Fig. 2: Uploading Time Comparison Graph**

**Table 2: Downloading Time Computation**

| File Size(KBs) | Two Pass Algorithm | DES Algorithm | Efficient Algorithm [6] |
|---|---|---|---|
| **50KB** | 0 | 1 | 2 |
| **100KB** | 0 | 1 | 2 |
| **200KB** | 1 | 2 | 4 |
| **500KB** | 2 | 4 | 5 |
| **1000KB** | 4 | 7 | 8 |
| **2000KB** | 7 | 14 | 15 |

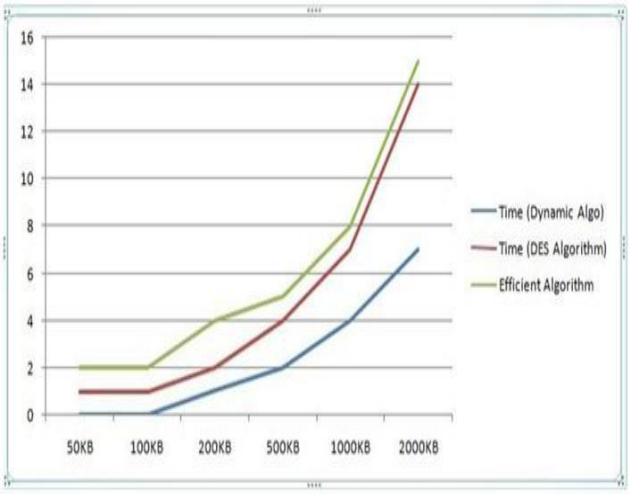


**Fig.3: Downloading Time Comparison Graph**

### C. Encrypted file size variation computation

For computing encrypted file size, we have taken all above file of size 50KB, 100KB, 200KB, 500KB, 1000KB and 2000KB, and applied encryption function of our algorithm and also applied encryption function of DES and Efficient algorithm on same data in same environment and stored results in Table-3. It is clear from the Table-3 that the file size which remain same before after in Two Pass Algorithm and in Efficient Algorithm but increases frequently in DES algorithm. It is also clear from Table-3 that file size increased drastically as plain file size increases, encrypted file size increasing factor is 39. A comparative Graph between encrypted file size of the algorithms has been shown in Fig. 4.

**Table 3: Encrypted File Size Comparison**

| File Size(KBs) | Two Pass Algorithm | DES Algorithm | Efficient Algorithm [6] |
|---|---|---|---|
| **50KB** | 50 | 69 | 50 |
| **100KB** | 100 | 140 | 100 |
| **200KB** | 200 | 279 | 200 |
| **500KB** | 500 | 697 | 500 |
| **1000KB** | 1000 | 1396 | 1000 |
| **2000KB** | 2000 | 2792 | 2000 |

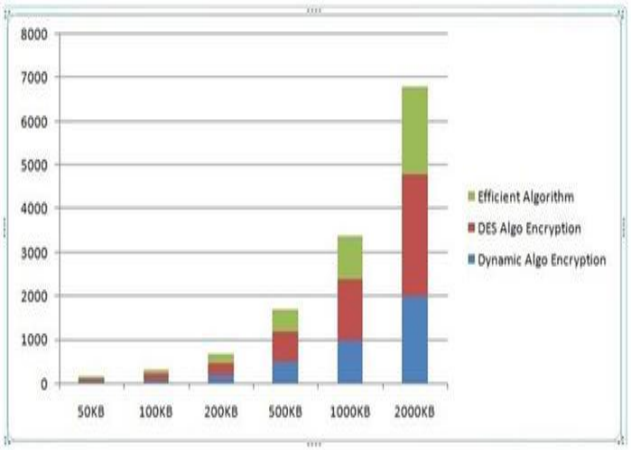


**Fig. 4: Encrypted File Size Comparison**

## VII. CONCLUSION AND FUTURE SCOPE

In this paper a Two Pass algorithm has been proposed which is data dependent and not user dependent which is producing key after analyzing data and encrypting according to the key produced and also testing integrity of the document while decrypting and taking necessary action if document is altered and also sensing which of the characters and consequently words have been affected and trying to rectify them. To the best of our knowledge so far no such type of Two Pass algorithm have been proposed and implemented. More over in this paper we have proposed an architecture which is dividing original files into multiple files and main advantage of this algorithm is that it will produce different key for each sub-file which decreases the probability of hacking or leakage of all data at once. If we do all this process by any other algorithm then it will encrypt all these sub-files by same keys or we have to change key for all sub-files or we need to use many algorithm for completing this task which is achieved by just a Two Pass Algorithm.

**Future scope** includes to compute the efficiency and then effectiveness of proposed algorithm in real environment and also to extend this concept for secure computation of data on cloud without user intervention. Moreover algorithms may be implemented on real platform like EC2 and S3 of AWS. Moreover if these two algorithms will be implemented in sequence, we can eliminate involvement of Third Party Audit as user himself or itself can audit its data.

## REFERENCES


1. L. Wei et al., "Security and privacy for storage and computation in cloud computing," *Information Sciences*, vol. 258, 2014, pp. 371–386.
2. Z. Deng, K. Li, K. Li, and J. Zhou, "A multi-user searchable encryption scheme with keyword authorization in a cloud storage," *Future Generation of Computer System.*, vol. 72, pp. 208–218, 2017.
3. H. Rasheed, "Data and infrastructure security auditing in cloud computing environments," *International Journal of Information Management*, vol. 34, no. 3, 2014, pp. 364–368.
4. L. T. Yang, G. Huang, J. Feng, and L. Xu, "Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud computing," *Information. Sciences (NY).*, vol. 387, 2017, pp. 254–265.
5. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM Journal Computer*, vol. 32, no. 3, 2003, pp. 586–615.
6. A. Azougaghe, Z. Kartit, M. Hedabou, M. Belkasmi, and M. El Marraki, "An efficient algorithm for data security in Cloud storage," *15th Int. Conf. Intelligent System. Design Application*, 2015, pp. 421–427.
7. Mohd. Tajammul, Rafat Parveen and Mohd. Shahnawaz. "Cloud Computing Security Issues and Methods to Resolve: Review", *Journal of Basic and Applied Engineering Research*, vol. 5, Issue 7; October-December, 2018, pp. 545-550.
8. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer. Applications*, vol. 34, no. 1, 2011, pp. 1–11.
9. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation of Computer System*, vol. 28, no. 3, 2012, pp. 583–592.
10. M. N. Manas, C. K. Nagalakshmi, and G. Shobha, "Cloud Computing Security Issues And Methods to Overcome," *International Journal of Advanced Research in Computer Communication. Eng.*, vol. 3, no. 4, 2014, pp. 6306–6310.
11. M. Armbrust et al., " A view of Cloud Computing," Communication of ACM, vol. 53, no. 4, 2010, pp. 50–58.
12. M. M. Potey, C. A. Dhote, and D. H. Sharma, "Homomorphic Encryption for Security of Cloud Data," Procedia Computer Science, vol. 79, 2016, pp. 175–181.

13. P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," *Procedia Computer Science*, vol. 125, no. 2009, 2018, pp. 691–697.
14. I. Chuang and S. Li, "An effective privacy protection scheme for cloud computing*," ICACT, 13th International Conference*, 2011, pp. 260–265.
15. Q. Wang, S. Member, C. Wang, S. Member, and K. Ren, "Enabling Public Auditability and Data Dynamic in Cloud Computing," *IEEE Trans. Parallel and Distributed System*, vol. 22, no. 5, 2012, pp. 847–859.
16. M. Mahindha, "Double Encryption Based Auditing Protocol Using Dynamic Operation in Cloud Storage", *International Journal on Recent and Innovation Trends in Computing and Communication* Volume: 5 Issue: 3, 2017, 294 – 299.
17. T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. K. Liu, "Towards secure and reliable cloud storage against data re-outsourcing*", Future Generation Computer System*, vol. 52, 2015, pp. 86–94.
18. Tajammul, M., Parveen, R., "Comparative Analysis of Big Ten ISMS Standards and their Effect on Cloud Computing", 978-1-5386-0627-8/17/$31.00c 2017 IEEE.
19. Tajammul, M., R. Parveen, "Comparative Study of Big Ten Information Security Management System Standards, *International Journal of Engineering Research in Computer Science and Engineering*, vol. 5, Issue 2, 2018, pp 2394-2320
20. S. L. Tim Mather, Subra Kumaraswamy, Cloud Privacy and Security, O'Reilly Publication, First Edition, p. 336.
21. Tajammul, M, Parveen, R. Cloud Computing Introduction to Innovation International Research Publication House, First Edition ISBN: 978-93-87388-31-4
22. M. Tajammul and R. Parveen, "Key Generation Algorithm Coupled with DES for Securing Cloud Storage," *International Journal of Engineering and Advanced Technology*, vol. 8, pp. 1452–1458, 2019.
23. Mohd Tajammul, Rafat Parveen, Cloud Computing: Introduction to Innovation, *International Research Publication House*, First Edition, p. 205.

## AUTHORS PROFILE

**Mr. Mohd. Tajammul holds M.Tech and pursuing PhD** in Computer Science from Department of Computer Science, Jamia Millia Islamia, New Delhi, India. He has more than 10 years of experience in teaching and research in the field of Computer Science. He has 10 publications including one book of his credit. He has taught more than 30 subjects of Computer Science. He has cracked UGC NET 4 times. His research interests include Cloud Computing, Cloud Storage, and Cloud Security. His recent publications includes in Scopus Indexed Database.

**Dr. Rafat Parveen PhD degree in Computer Science** from Department of Computer Science, Jamia Millia Islamia, New Delhi, India. She has more than 20 years of experience in teaching and research in the field of Computer Science in National and International Universities. She has 30 publications including books of her credit. She has taught more than 35 subjects of Computer Science. Her research interests include Bioinformatics, Lever Cancer, Cloud Computing, Cloud Storage, and Cloud Security. Her recent publications includes in Scopus Indexed Database. She has guided a no. of students in various projects. Moreover she has guided 8 students for PhD in Computer Science.