International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

Key Generation Algorithm Coupled with DES for Securing Cloud Storage

Mohd. Tajammul, Rafat Parveen

Abstract: ***Cloud computing is a very fruitful technology providing uncountable services to the customers on pay per use basis. Many popular companies are offering cloud services in modern age of data and computation. Whenever a user transfer his data on cloud for computation or just for storing purpose, this data comes under the eyes of man-in-the-middle, Cloud Service Provider (CSP) and internal employees of CSP. Sudden attack on cloud storage in 2014 shows that the cloud is still in its early stage as 50 million users' accounts were hacked in the attack. Lots of companies are there in market like Amazon Web Services (AWS) providing computation and storage but fear of hacking remains in the mind of data owner. Lots of algorithms have already been designed in this field but all of them seek for user to enter key. This research paper proposed a key generation algorithm which is coupled with Data Encryption Standard (DES) for generating unique key itself and subsequently encrypts data on the basis of key produced. The plus point behind designing this algorithm is not only to develop an automatic system which itself produce key for encryption but also making this complete process user independent. User need to upload the text data only, the key produced will be sent to user related to that particular data and encrypted data will be uploaded on cloud storage. The algorithm can be utilized in making cloud storage as a secure place to store data as well as it can be utilized while sending data outside boundaries of your organization.***

Index Terms: Cloud Computing, Cloud Storage, Cloud Computation, Cloud Security

I. INTRODUCTION

Cloud computing is a fruitful technology offering numerous services to the users on demand at remote location and follow pay as you go rule. Going into details we will find that it is not a separate technology in itself rather it is a collection of many technologies integrated together to take combined advantage of various technologies simultaneously. Technologies involved in cloud computing are parallel computing, distributed computing, virtualization and Internet. Out of these technologies, Internet is considered as backbone of cloud computing because cloud services are accessible only through Internet [10]. Cloud computing is very rich in its definitions. There are lots of definitions of cloud computing. We are discussing some of standard definitions here. First of all the term cloud computing was pronounced by Professor John Mc. Carthy, he defined cloud computing in his tongue as: " If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility, this computer utility could become the basis of a new and important industry" [10, 14, 18].

Douglas Parkhill defined cloud computing with its features in the book 'The Challenge of the Computer Utility' in 1966 as: "Cloud computing is super-set of Virtual Private Network (VPN) along with network infrastructure that is utilized by telecommunication". NIST (National Institute of Standards and Technology) defined cloud computing as: "a model for enabling convenient, on demand network access to a shared pool of configurable 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" [10].

A. Deployment Models Of Cloud Computing

There are four deployment models of cloud computing. These models are private cloud, public cloud, hybrid cloud and community cloud. These models are deployed as per requirements of users. If any of the users wish to access a cloud without sensitive data he or she is advised adopt public cloud, on the other hand if somebody wish to store or compute his or her sensitive data, best solution for such a customer is private cloud and if somebody wants to take benefits of two clouds simultaneously, he or she can adopt hybrid cloud. Apart from this if there are some known to enterprises and want to involve in computation, they should adopt community cloud. Total capacity of this cloud will be available only for those organizations which are known to each other. These four types of deployment models of cloud computing are discussed as:

- **Private Cloud** - This model is available only for individual or for particular organization that to store sensitive secure or data on it. This model is completely owned by particular individual specific organization or by. The whole functionality of this cloud will be usable for somebody who owned it [14].
- **Public Cloud** - This is a simplest model of cloud computing. It is accessible to all publically. If the data, we required to compute or store on cloud storage is not sensitive, we can use this cloud model [14].

Manuscript published on 30 June 2019.
* Correspondence Author (s)
Mohd. Tajammul, Department of Computer Science, Jamia Millia Islamia, New Delhi, India.
Rafat Parveen, (Corresponding Author) Department of Computer Science, Jamia Millia Islamia, New Delhi, India.

• **Hybrid Cloud** - This cloud is designed by combining the features of of two or more clouds. This is suggested in situation where one cloud is unable to fulfill the needs of users. Advantages of designing this cloud are as: it is helpful for heterogeneous types of needs of users which are beyond the capability of just one cloud [10].

• **Community Cloud** - When some trusted parties or some trusted organizations develop their cloud and the whole strength of the cloud is usable only for these organizations, such cloud is treated as community cloud [18].

Before adopting anyone of the above models for computation or for storing data, it is advised to test the nature of the data first and then go for adoption of cloud because of a no. of security challenges and issues which must be kept in mind to avoid any type of data breaches and hacking. The service model stack of cloud computing has been given in Fig. 1.

B. Service Models of Cloud Computing

There are three service models of cloud computing namely SaaS(Software as a Service), PaaS(Platform as a Serivice) and IaaS(Infrastructure as a Service). These models are discussed as:

• **Software-as-a-Service** - This model is an upper most service model of cloud computing. In this model, software is offered to the cloud customers. Maintenance of the software is carried out on provider's side, users can use but cannot make any change in it. Many organizations are providing SaaS. Some popular of them are as: SalesForce.com, IBM NetSuite, Microsoft and Oracle [18].

• **Platform-as-a-Service** - This model is considered as middle model in cloud architecture. The model is available for those who want to begin their own company having no proper equipment. This model provides a platform to the users or to the clients by using which they can develop their applications. For instance: a business minded wish to start software development company having only laptops and no proper platform on which he can develop software. PaaS is available for such people. Some popular companies, offering PaaS are as: Microsofts Azure and GAE [18].

• **Infrastructure-as-a-Service** - This model is lowest service model in cloud computing architecture. In this service model an infrastructure is reserved for the customers for and they are charged on pay-per-use basis. For instance: if somebody wish to keep his data beyond the boundary of his organization, he can go to CSP for storage as a service or if somebody wish to perform computation which is beyond the control of single node, he can go to CSP for computation as a service. In both of cases, they will be provided services on the basis of SLA (Service Level Agreement) and will be charged for the time they use service. Famous IaaS providers are as: Joyent, Flexiscale, GoGrid, and Rackspace [18].

C. Salient Characteristics of Cloud Computing

Cloud computing supports in growth that ranges from common man to large scale organization by offering numerous as well as cheap and best services. There are a no. of features of cloud computing. Let's list out some of popular of them:

- Resource pooling
- Measured service
- 24X7 on demand service
- Broad network access
- Pay per use service and cost effective
- Rapid elasticity [1, 6]

D. Issues And Challenges of Cloud Computing

In its initial stage, market of cloud computing was growing rapidly because of few challenges on those days. But the time by which cloud it spread in all directions, issues and challenges grew rapidly. Out of many challenges some important are discussed here:

- Performance
- Privacy and security
- Power consumption
- Elasticity and scalability
- Portability and interoperability
- Resource provisioning and management
- Availability and reliability [14, 18]

Out of these issues and challenges, in second point we have seen an issue of security and privacy. This paper has been written from the aspect of security, therefore we will discuss this issue in details here:

- Data confidentiality
- Authentication
- Maintaining integrity
- Web application security
- Data breaches
- Network security
- Data security
- Sign-on process and identity management
- Data access
- Availability
- Data segregation
- Backup and recovery
- Data locality [14, 18]

Here, we have seen that there are a no. of security issues related to data in the field of cloud computing. Whenever we transmit data to the cloud either for computation or for storing purpose only, this data needs a lot of attention in terms of security. It is highly risky to upload data on cloud in its plain form [2]. Therefore it is common intelligence to encrypt the data before uploading it on to cloud space. Many algorithms are available for securing data by encrypting it. Out of those some popular algorithms are Data Encryption Standard (DES), Advanced Encryption Standard (AES), BlowFish, Rivest Shamir Adleman (RSA), International Data Encryption Algorithm (IDEA). On cloud we use homomorphic or symmetric algorithm to encrypt data [3]. The meaning of homomorphic in cloud is straight forward. It means that the encryptor and decryptor will be the same person. Some of the authors are using concept of double encryption to encrypt data [7]. They encrypt data by using one algorithm and again encrypt the pre-encrypted file by using the same or different algorithm. Some others are encrypting the data by one algorithm and again encrypting the key by different algorithm and storing data on cloud and encrypted key on local storage to keep both data and key secure [13].

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

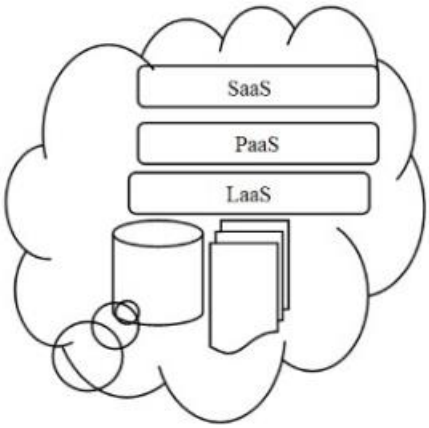

Fig.1: Cloud Computing

E. Our Contribution

In this research paper, we have learnt how to design and develop an algorithm based on matrices rather than group. Here, we have proposed an algorithm which will sense the input data automatically and will generate the encryption key in matrix form. Our main objective is to utilize multidimensional key rather than single dimensional. This is first attempt to go towards the matrix approach and non linear key. We have designed an algorithm that is key generation algorithm integrated with DES for encryption and decryption. Our contribution has been summarized as under:

- **Firstly,** we have designed an algorithm which will generate the key on reading or sensing the input data. This key generation makes user free for generating or creating key for encryption. Each and every time key produced will be unique and dynamic. If data is different than key is different.
- **Secondly,** we have integrated this key generation algorithm with the DES (Data Encryption Standard) algorithm for encryption and decryption. Our main motto behind encryption decryption is to make data secure before uploading it on cloud storage because cloud storage is not as secure as our desktop systems.
- **Thirdly,** we have designed architecture of the proposed system to make things easier to understand. This architecture shows the flow of information from user to cloud and from cloud to user in secured and efficient way.
- **Fourthly,** we have computed the result for checking the efficiency of proposed work. In this work we have computed time taken for key generation as well as time taken for encryption and decryption. For performing this experimental work we have collected data ranges from 500KB to 5000KB. Nature of the data with size as well as source has been shown in Table 1.

Rest of this paper is organized as: Section 2 discussed Related Works, Section 3 discussed Motivation and Research Gap, Section 4 Proposed Algorithm, Section 5 Data Collection, Section 6 Experiments and Result Calculation and Section 7 concludes the paper with future research directions.

II. RELATED WORKS

Hassan Rasheed, 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 [10]. Mohd. Tajammul and Rafat Parveen discussed big ten ISMS standards and their effects on cloud computing [14]. 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 [15]. 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 [1]. Zuojie et al. proposed a scheme for multitenant environment to search with authorized keyword. This solves the problem of finding encrypted files on storage in cloud computing [9]. 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 [8]. 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 [11]. Dimitrias Zissis, Dimitrias Lekkas addressed cloud security issues in tabular form representation by discussing levels of security users and security requirements and threats also [16]. 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 [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 [3]. P. Ravi Kumar et al. Discussed various data security issues as well as resolution technique in cloud computing [4]. 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 [13]. 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 [2]. 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 [5]. 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 [7]. Qian Wang et al. Tried to enable public auditability as well as data dynamics for cloud storage. Authors discussed integrity, public auditability and dynamic data operations [6].

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

III. Motivation and Research Gap

On reviewing the available literature, it is clear that for storing or computing data on cloud, we need to encrypt it for avoiding any breaches. To encrypt data we apply any of encrypting algorithms and produce Cipher text. Suppose we reserved some space on cloud for storing our valuable data on it. Each time we enter key in algorithm. Now suppose we upload 100 of documents on cloud storage and each of documents was encrypted by same key, if this key is stolen by someone, it is easy for him to crack each and every document very easily.

To avoid this problem we need to design a strategy which produce unique key for each document and start encryption according to that. If in future somebody steals this key, he can only decrypt just one document out of 100 of documents. Moreover if he will again try to decrypt any other document by the same key, he would not be able to do so at any cost. By doing this we can save rest of the documents. In previous case there was possibility to decrypt all the documents with just one key but proposed strategy reduces this possibility to just one document. Two questions have been set as guidelines to fulfill this aim.

1. *How to produce a unique key for each document?*

2. *How to overcome from the problem of stealing all the data at once?*

3. *How to pass this unique key to encryption algorithm and to user of the data?*

This research paper is an attempt to answer the above said questions and to fulfill the research gap which has been discussed earlier.

IV. Proposed Algorithm

Proposed algorithm has been designed in two phases. In first phase document is read and key is generated. This key it passed to the DES along with document which is second phase of the algorithm. A conceptual framework of the algorithm has been given in Fig. 2.

In this figure data file will be given to key generation algorithm as an argument. On the basis of sensing the data given in input file, key generation algorithm produces a key. This key in turn is passed to DES (Data Encryption Standard) with Input as arguments. Using these arguments DES produces encrypted file. This file is uploaded on cloud storage and key is stored locally.

At the time of downloading encrypted file is downloaded from cloud storage, key is extracted from local storage and DES is applied to decrypt the data and decrypted file is stored. Our main motto to store encrypted file on cloud storage is just because there are a no. of hackers and internal employees and moreover CSP (Cloud Service Provider). Due to deficiency of storage, somehow we have to upload our data on cloud storage. Encryption saves our data from hacking and fraud utilization.

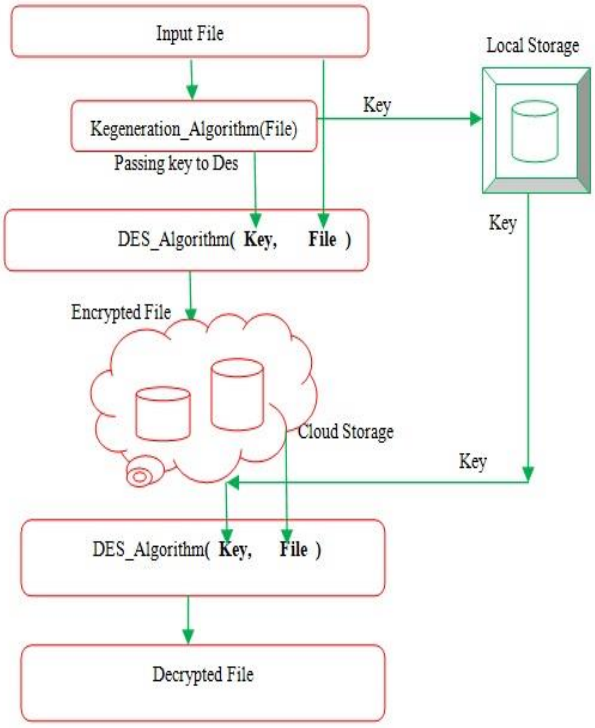

Fig.2: Proposed framework of the system

A. Algorithm: Key Generation Encryption Algorithm

Input: *Φ as Plain Text*
Output: *Key, Ψ as Encrypted Text and Decrypted Text*
Call *KeyGeneration(Φ)* ***Method***

1. *Integer i= 0; j= 0 // Phase I*
2. *A←Char_Frequency( )//Count occurrences of all char*
3. *p←Random_Prime 29 <= p <=97*
4. *B ←A%p // Taking remainder division of A by prime p*
5. *C←Char (B+ASCII_Values (a to z; 0 to 9))// no. to ASCII*
6. *D←alphabet Such that L(alphabet) not equals to L(Φ)*
7. ***while i < 6 do***
8. ***while j < 6 do***
9. ***if (C has duplicate entries) then***
10. *C_dupliEntries ← D_corresEntries*
11. *E ←C*
12. ***else***
13. *E ←C*
14. ***end***
15. *++ j*
16. ***end***
17. *++i*
18. ***end***
19. *Key←F ←Transpose(E)// E's Transpose stored in F, Key*
20. *Pass key to DES as well as store at local server*
21. *Ψ← **DES_Encrypt**(Key, Φ)// Phase II*
22. *Upload Ψ on cloud storage*
23. *Extract Key from local server and download Ψ from cloud storage*
24. *Φ← **DES_Decrypt**(Key, Ψ)*
25. *Finish*

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

In above algorithm A, B, C, D, E, F are matrices of 6X6 each, p is a random prime no. having value between 29 and 97. KeyGeneration ( ) method generate key on reading input file and by executing steps from 1 to 19. Char_Frequency( ) method computes the frequency of each alphabet including 0 to 9 and store in matrix A. L stands for language. L(alphabets) not equals to L(Φ) means language of alphabets and language of Φ both are different. For example if language of input file is 'English', the language of alphabets stored in matrix D will be different from 'English', it may be any other language like 'Arabic' or 'Hindi', 'Punjabi' etc. Transpose(E) method, transpose matrix E and store result into F and subsequently in Key.

Matrix C will have duplicate entries. To remove these duplicate entries, we have designed another matrix D, this matrix is an alphabet matrix having unique alphabets. The procedure of removing duplicates from matrix C is very simple. First of all a comparison among the elements of matrix C will carry out. During comparison if an element have its duplicate then it is replaced by corresponding position element of matrix D. This method is repeated until and unless all the elements in matrix C become unique. The main benefits behind the elements of matrix C to be unique are as the encryption for each document will be unique and dynamic.

B. Pseudo code for DES Cipher_Text[17]

```
Cipher_Text (plainTextBlock[64], RoundsKeys[16, 48],
Cipher_TextBlock[64])
{
 permute (64, 64, plainTextBlock, inBlock,
InitialPermutationTable)
 split (64, 32, inBlock, leftBlock, rightBlock)
 for (rounds= 1 to 16)
 {
 mixer (leftBlock, rightBlock, RoundsKeys[round])
 if (round!=16) swapper (leftBlock, rightBlock)
 }
 combine (32, 64, leftBlock, rightBlock, outBlock)
 permute (64, 64, outBlock, Cipher_TextBlock,
FinalPermutationTable)
}
mixer (leftBlock[48], rightBlock[48], RoundsKey[48])
{
 copy (32, rightBlock, B1)
 method(B1, RoundKey, B2)
 exclusiveOr (32, leftBlock, B2, B3)
 copy (32, B3, rightBlock)
}
swapper (leftBlock[32], rigthBlock[32])
{
 copy (32, leftBlock, B)
 copy (32, rightBlock, leftBlock)
 copy (32, B, rightBlock)
}
method (inBlock[32], RoundsKey[48], outBlock[32])
{
 permute (32, 48, inBlock, B1, ExpansionPermutationTable)
 exclusiveOr (48, B1, RoundKey, B2)
 substitute (B2, B3, SubstituteTables)
 permute (32, 32, B3, outBlock, StraightPermutationTable)
}
substitute (inBlock[32], outBlock[48], SubstitutionTables[8,
4, 16])
{
 for (i = 1 to 8)
 {
 row ←2X inBlock[i X 6 + 1] + inBlock [i X 6 + 6]
 col ←8 X inBlock[i X 6 + 2] + 4 X inBlock[i X 6 + 3] +
 2 X inBlock[i X 6 + 4] + inBlock[i X 6 + 5]
 value = SubstitutionTables [i][row][col]
 outBlock[[i X 4 + 1] ←value / 8; value ←value mod 8
 outBlock[[i X 4 + 2] ← value / 4; value ← value mod 4
 outBlock[[i X 4 + 3] ←value / 2; value ← value mod 2
 outBlock[[i X 4 + 4] ← value}}
```

C. Advantages of algorithm

- Algorithm reduces the hacking possibility
- Algorithm reduces the time of entering key and reduces possibility of stealing key and subsequently breaches of data
- Algorithm increase the security by encryption
- Each time key is unique and non linear

V. Data Collection

To execute the algorithm, we have collected online data from two locations. Data that we collected from both the sources is free from pictures and is in textual form only. download/ and https://archive.ics.uci.edu/ml/index.php https://file-examples.com/index.php/text-files-and-archives- for more specific and detailed information, we are creating a table which shows data source, type and size.

Table 1: Data Type and Size

Data Type	Data Source	Data Size
Textual	UCI MLR	100KB
Textual	UCI MLR	200KB
Textual	UCI MLR	500KB
Textual	UCI MLR	1000KB
Textual	UCI MLR	2000KB
Textual	Examples.com	50KB

Note - UCIMLR-UCI Machine Learning Repository

VI. Experiments and Result Calculation

For calculating the efficiency of proposed algorithm, we have developed an application in java that simulates the behavior of algorithm. The application was developed in java having version JDK1.6.0, NetBeans IDE with version 7.2.1 and Notepad++, on Intel Core i3-5005U CPU @ 2.00GHz, 1TB HDD, 8GB RAM, 64 bit Windows Pro Operating System. All experiments were executed 10 times on single threaded machine. Performance of the algorithm was measured against time Vs file size. Results of experiments are given in Table 1. Data on which experiments were performed ranges from 50 KB to 2000 KB.

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

Table 1: Time Taken in Key Generation

File_Size	Time taken for Key Generation
50 KB	Lt 1Second
100 KB	Lt 1Second
200 KB	Lt 1Second
500 KB	Lt 1Second
1000 KB	1Second
2000 KB	1Second

Note – Lt denotes Less than in above table

Table 2: Time taken in Encryption and Decryption

File_Size	Encryption_Time	Decryption_ Time
50 KB	2 Seconds	2 Second
100 KB	3 Seconds	2 Seconds
200 KB	4 Seconds	3 Seconds
500 KB	8 Seconds	5 Seconds
1000 KB	15 Seconds	9 Seconds
2000 KB	27 Seconds	16 Seconds

It is clear from the Table 1, the time taken by algorithm in encryption of data is more than that decryption because in encryption phase, algorithm takes some time to generate key. On the basis of results computed by performing experiments, a comparative graph has been sketched for encryption and decryption time against data in Fig.3 as under.

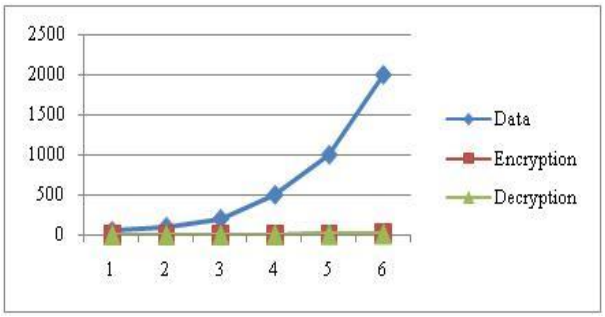

Fig.3: Encryption and Decryption time against Data

VII. CONCLUSION AND FUTURE SCOPE

In this research paper, we have proposed an algorithm which will generate key on reading data input. This key is passed to DES (Data Encryption Standard) algorithm which will encrypt the given data according to key produced in first phase. The concept of the algorithm resembles to the concept of two pass compiler as the code produced by two pass compiler is always good in quality. Similarly the encrypted file produced by this algorithm is also good in quality. In first phase algorithm sense the document and produce the key while in second phase it encrypt the data on the basis of key produced. The algorithm reduces the possibility of hacking all data because of generating unique key for each document. Moreover algorithm stores the generated key into a separate file on local server so that for decrypting the data, this key may be referenced in future. We can conclude that the algorithm save the documents from unauthorized changes while saving user's time side by side on sensing document and by producing key itself. Final matrix E is not used as key rather its transpose is computed to make data more and more secure.

Future work in this field is to implement this algorithm in real environment and to compute its performance against big data. Apart from this the given algorithm may be further enhanced to reduce its time complexity and to increase its efficiency. The algorithm can also be expended for secure migration of cloud data from one CSP (Cloud Service Provider) to other. More over the algorithm can be enhanced for key management because multiple documents, multiple key will be produced according to one key per document.

REFERENCES

1. M. N. Manas, C. K., Nagalakshmi, & G. Shobha., "Cloud computing security issues and methods to overcome". *International Journal of. Advanced Research in Computer and Communication Engineering*, vol. 3, no. 4, 2014, pp. 6306–6310.
2. M. Armbrust et al., "A view of cloud computing", *Communication ACM*, vol. 53, no. 4, 2010, pp. 50–58.
3. 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.
4. P. R. Kumar, P. H. Raj, & P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing" Procedia Computer Science, vol. 125, no. 2009, 2018, pp. 691–697.
5. I. Chuang and S. Li., "An effective privacy protection scheme for cloud computing", *Proceeding of 13th International conference ICACT*, pp, 2018, 260–265.
6. Q. Wang, S. Member, C. Wang, S. Member, & K. Ren, "Enabling public auditability and data dynamic in cloud computing", *IEEE Transactions Parallel Distributed. System*, vol. 22, no. 5, 2010, pp. 847–859.
7. M. Mahindh, "Double encryption based auditing protocol using dynamic operation in cloud storage", *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 5, 2017, pp. 294-299.
8. L. Wei et al., "Security and privacy for storage and computation in cloud computing", *Information Sciences*, vol. 258, 2014, pp. 371–386.
9. Z. Deng, K. Li, K. Li, and J. Zhou, "A multi-user searchable encryption scheme with keyword authorization in cloud storage", *Future Generation Computer Systems*, vol. 72, 2017, pp. 208–218.
10. H. Rasheed, "Data and infrastructure security auditing in cloud computing environments", *International Journal of Information Management*, vol. 34, no. 3, 2014, pp. 364–368.
11. 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*, vol. 387, 2017, pp. 254–265.
12. D. Boneh and M. Franklin,"Identity-Based Encryption from the Weil Pairing", *SIAM Journal of Computing*, vol. 32, no. 3, 2013, pp. 586–615.
13. A. Azougaghe, Z. Kartit, M. Hedabou, M. Belkasmi, and M. El Marraki "An efficient algorithm for data security in cloud storage", *Proceeding of 15th International Conference on Intelligent System Design Application*, 2015, pp. 421–427.
14. M. Tajammul, R. Parveen, "Comparative analysis of big ten ISMS standards and their effect on cloud computing", IEEE Explore, 2017, 978-1-5386-06278/17/$31.00
15. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of Network Computer Application*, vol. 34, no. 1, 2011, pp. 1–11.
16. D. Zissis and D. Lekkas, "Addressing cloud computing security issues", *Future Generation Computer Systems*, vol. 28, no. 3, 2012, pp. 583–592.
17. https://academic.csuohio.edu/yuc/security/Chapter_06_Data_Encriptio n_Standard.pdf
18. M. Tajammul, R. Parveen, Shahnawaz, "Cloud computing security issues and methods to resolve: Review", Journal of Basic and Applied Engineering Research, Vol. 5, Issue 7, 2018, pp. 545-550

19. Parveen, R. & Tajammul, M. (2017). Comparative Analysis of Big Ten ISMS Standards and Their Effect on Cloud Computing, International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), 978-1-5386-0627 8/17/31:00c2017IEEE; 9001; 362367.
20. Mohd. Tajammul, Rafat Parveen, "Auto Encryption Algorithm for Uploading Data on Cloud Storage", BIJIT - BVICAM's International Journal of Information Technology ISSN: 2511-2104 (print version), in press.
21. Mohd. Tajammul, Rafat Parveen, "Two Pass Multidimensional Key Generation and Encryption Algorithm for Data Storage Security in Cloud Computing", International Journal of Engineering Research and Technology ISSN:09743154, Scopus Indexed, in press.
22. Mohd. Tajammul, Rafat Parveen, "Algorithm for Document Integrity Testing Pre Upload and Post Download from Cloud Storage" International Journal of Recent Technology and Engineering ISSN:22773878, Scopus Indexed, in press.
23. M. Tajammul, R. Parveen, and M. Shahnawaz, "Cloud Computing Security Issues and Methods to Resolve : Review," vol. 5, no. 7, pp. 545–550, 2018.
24. Tajammul M., Delhi, N. (2018). Comparative Study of Big Ten Information Security Management System Standards, International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 2, February 20185(2), 514.
25. Parveen, R. & Tajammul, M. (2017). Comparative Analysis of Big Ten ISMS Standards and Their Effect on Cloud Computing, International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), 978-1-5386-0627 8/17/31:00c2017IEEE; 9001; 362367.
26. Mohd. Tajammul, Rafat Parveen, "Auto Encryption Algorithm for Uploading Data on Cloud Storage", BIJIT - BVICAM's International Journal of Information Technology ISSN: 2511-2104 (print version)-, in press.
27. Mohd. Tajammul, Rafat Parveen, "Two Pass Multidimensional Key Generation and Encryption Algorithm for Data Storage Security in Cloud Computing", International Journal of Engineering Research and Technology ISSN:09743154, Scopus Indexed, in press.
28. Mohd. Tajammul, Rafat Parveen, "Algorithm for Document Integrity Testing Pre Upload and Post Download from Cloud Storage" International Journal of Recent Technology and Engineering ISSN:22773878, Scopus Indexed, in press.
29. M. Tajammul, R. Parveen, and M. Shahnawaz, "Cloud Computing Security Issues and Methods to Resolve : Review," vol. 5, no. 7, pp. 545–550, 2018.
30. Tajammul M., Parveen, R. Delhi, N. (2018). Comparative Study of Big Ten Information Security Management System Standards, International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 2, February 20185(2), 514.
31. Rafat Parveen, (2017) Early prediction of Lungs Cancer Using Systems Biology communicated , IEE Journal of Systems Biology
32. Parveen, R. & Raza, K. (2013). Reconstruction of gene regulatory network of colon cancer using information theoretic approach. In Proc. of 4 th International Conference (CONFLUENCE-2013): The Next Generation Information Technology Summit, 26-27 Sept., 2013, p. 461-466. doi: 10.1049/cp.2013.2357 (IEEE Xplore & IET Digital Library).
33. Raza, K. & Parveen, R. (2012). Soft computing approach for modeling genetic regulatory networks. Advances in Intelligent Systems and Computing, 178, 1-11, Springer-Verlag Berlin Heidelberg, doi: 10.1007/978-3-642-31600-5_1
34. Raza, K. & Parveen, R. (2012). Evolutionary algorithms in genetic regulatory network model. Journal of Advanced Bioinformatics Applications and Research, 1(3), 271-280. (Global IF 1.057)
35. Rafat Parveen, Simulation of Regulatory Networks,WORLDCOMP,International Conference,USAJuly 17-21,2011
36. Rafat Parveen ,Read I.Hamed and Prof.Syed I.Ahson. Modelling Cellular Process of the Eukaryotic DNA Using Hybrid Functional Petri Nets, International Journal of Bioinformatics, ISSN:0974-6439, Vol. 1(2), pp. 55-56. July-Dec,2008
37. Rafat Parveen ,Read I.Hamed and Prof.Syed I.Ahson, A new approach for Modeling Gene Regulatory Networks Using Fuzzy Petri Nets.Journel of Integrative Bioinformatics(JIB), Vol 7(1):113,p.p.1-16,2010,Germany
38. Rafat Parveen ,Read I.Hamed and Prof.Syed I.Ahson,Petri Nets Modeling and Simulation of Transcriptional Regulation in E.Coli.A Journel of Bioinformatics and its Applications ,Bioinformatics Trends;Vol(2 & 3),pp.87-91,2009
39. Rafat Parveen ,Read I.Hamed and Prof.Syed I.Ahson,Designing Genetic Regulatory Networks Using Fuzzy Petri Nets Approach (IJAC),Springer-Verlag Berlin Heidelberg, Vol 7(3),pp403-412,2010

AUTHORS PROFILE

Mr. Mohd. Tajammul , BSc. B. Ed. MCA, M. Tech, PhD Pur. Research Scholar, Deptt. of Computer Science, Jamia Millia Islamia, New Delhi
mohammad8002@gmail.com

Author has presented/published a no. of papers in international journals as well as conferences. He is having 10 years of teaching and research experience. Some of his research work is listed here:

Dr. Rafat Parveen, BSc, MSc, M.Tech, PhD Associate Professor, Deptt. of Computer Science, Jamia Millia Islamia, New Delhi
rafatparveenjmi@gmail.com

Author has presented/published a no. of papers in international journals as well as conferences. She is having 20 years of teaching and research experience with national and international universities. Some of her research work is listed here: