International Journal of Engineering & Technology, 7 (1) (2018) 223-227

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i1.9309
Research paper

Data encryption in public cloud using multi-phase encryption model

Snata Choudhury [1]*, Kirubanand V.B [2]

[1]Computer Science Department, Christ University, Student,Bangalore, India
[2] Computer Science Department, Christ University, Professor,Bangalore, India
**Corresponding author E-mail: snatachoudhury16121993@gmail.com*

Abstract

Cloud computing the most used word in the world of Information Technology, is creating huge differences in IT industry. Nowadays huge amount of data is being generated and the researchers are finding new ways of managing these data. Basically, the word cloud refers to a virtual database that stores huge data from various clients. There are three types of cloud public, private and hybrid. Public cloud is basically for general users where users can use cloud services free or by paying. Private cloud is for any particular organizations and hybrid one is basically combine of both. Cloud offers various kind of services such as IAAS, PAAS, SAAS where services like platform for running any application, accessing the huge storage, can use any application running under cloud are given. The cloud also has a disadvantage regarding the security for the data storage facility. Basically, the public cloud is prone to data modification, data hacking and thus the integrity and confidentiality of the data is being compromised. Here in our work the concern is to protect the data that will be stored in the public cloud by using the multi-phase encryption. The algorithm that we have proposed is a combination of Rail Fence cipher and Play Fair cipher.

Keywords: *Cloud Computing; Cryptography Algorithm; Security Issues; Multiphase Encryption.*

1. Introduction

1.1. Cloud computing

Cloud Computing is a platform with so much IT related services. Cloud platform offers services like as a platform to deploy any applications, offers solutions, offers massive storage area and also helps in hosting purpose too. Cloud Computing is a versatile platform where based on the needs services can accessed by paying minimum amount or at free of cost. It offers various different types of clouds like public, private and hybrid cloud based on security purpose and also based on the needs of each user. The basic cloud architecture consists of three parts: Essential Characteristics, Service models, Deployment models. The essential characteristics includes: Broad Network Access, Rapid Elasticity, Measured Service, On-Demand Self Service, and Resource Pooling. Service Models includes: Platform as a service (PAAS), Software as a service (SAAS), and Infrastructure as a service (IAAS). Deployment model includes several varieties of clouds: Private cloud, Public cloud, Hybrid cloud and Community cloud. The IAAS offers platform, storage, network and other fundamental resources. Here the consumer can deploy an application and have total control over the operating system, storage and deployed application. The PAAS offers platform for deployment. Here the consumer can control only the deployed application. The SAAS offers to use any application running on cloud platform. In public cloud we can see that data from various users can be stored. The users here are the general people. The general users or consumers can pay minimum amount to use the cloud services. The private cloud is mainly for a particular organization and their cloud network can only be accessed within their organization. These private organizations will also pay a minimal amount to use the cloud service. The hybrid cloud is actually made up of public and private clouds. Highly changeable workloads require this. The community cloud is basically for a particular community-based organization. Thus, in this way data can be stored, used and how applications can be run in a cloud network. Simultaneously all this data that are being stored is not at all safe and secured because there is no particular security mechanism for this. The cloud data is very much vulnerable to Data breaching, Data loss, Data modifications, DOS attacks, Malware attacks, Data stealing, Hacked API, Broken credentials and authentication, APT parasite, Shared technologies and shared dangers. So, to secure the data from hacking we need to encrypt it by using encryption algorithms.

1.2. Cryptography

Cryptography is the method for encrypting data such that the outsider cannot get in contact with the real data. Cryptography is the method of transforming the actual data into a gibberish or unreadable format. Cryptography is used when a sender sends some data to the receiver and when the data is vulnerable to attack and modification from outsider then it helps to encrypt the data into cipher text and this data is being sent to the receiver. This cipher form is again being decrypted into the original form at the receiver’s side. There are two methods for cryptography and those are Symmetric and Asymmetric methods. Symmetric method is nothing but where a single key is being used to encrypt the original data to cipher form before sending the data over network. This key is called the public key. This method also has some drawbacks because the single key is hack able and thus data can be modified. So Asymmetric method came into picture. Here instead of a single key, both public key and private key are used. The sender’s content is enciphered using the public key and can only be deciphered using the private key of the receiver. This method of encryption is doubly protected and is one of the safest encryption methods. Thus, by using these methods data in the cloud can be encrypted as well as decrypted.

This paper proposes a new hybrid encryption method. This multi-phase encryption consists of two phases and these are: 1. Rail-fence cipher and 2. Play-fair cipher, methods. Basically, the original data that will be uploaded into the cloud will be first going through the Rail-fence encryption and then the second phase encryption will be done by Play-fair cipher. This final data will be uploaded into the cloud. In case of decryption, firstly Play-fair cipher will be decrypted, and then Rail-fence cipher will be decrypted. Finally, the original data will be retrieved.

The rest of the paper includes description about related research works done, description about the algorithms to be used, description about the proposed structure along with results and example, and finally conclusion with future scope and limitations are also described.

2. Related work

The idea for my work is being inspired from some previous work where some methods of securing data is being stated and some works dealt with the detailed study of the encryption methods and security threats in cloud. The following are the review of some related works:

Shakeeba S. Khan, Prof.R.R. Tuteja [1], have stated in their paper that Cloud computing is a network where storage, hardware, software and other resources are being provided to the consumers to store, deploy applications. They also stated that cloud has so many benefits that include scalability, cost effective, reliability, resilience and also, we don’t have to carry extra hard-drives for storage. In order to secure the data in the cloud server they have proposed a double-encryption method. Their method is the combination of the DES (Data Encryption Standard) and RSA algorithms. They have given a two-phased encryption method for encrypting the data before uploading the data in the server.

P.Subhasri and Dr.A.Padmapriya [2], have stated in their paper that Cloud computing is a flexible technology that helps to allocate resources to the users on their demand. The more the cloud technology is improving the more security issues are coming up. The data is being compromised and so they have stated that a method for encrypting the data. They have stated a multi-encryption method that combines Rail-fence cipher and Caesar cipher to encrypt the data before uploading it into the public cloud server.

Karun Handa and Uma Singh [3], have stated in their paper that Cloud computing is a mode of getting resources on demand. Thus, the resources are available anytime and anyone can access the resources anytime. This may be an advantage due to the demand-based resource availability but at the same time there is a high risk of data hacking too. The data that we are storing in the remote servers can be modified anytime because there is no mode of security while uploading it. Thus, they have come up with a new and innovative way for storing the data. Their work consists of the combination of cryptography and steganography methods to secure the data that are uploaded.

Treesa Maria Vincent and Mrs. J. Sakunthala [4], have stated in their paper that Cloud computing is a platform for getting resources on-demand. It’s a platform where we can store and access the data anytime but at the same time this data can be hacked anytime due to less security measures. So, the authors have proposed a new idea for safeguarding this data. The method is called the One-to-many order preserving mapping technique. Here Relevance score is used for indexing purpose. Searchable encryption technique that supports Boolean search process is also is in use.

Ming Li, Shucheng Yu, Ning Cao and Wenjing Lou [5], have stated in their paper that in cloud computing clients basically store data in the cloud server and the resources can be outsourced and can be got based on their demand but this data is not at all safe in the server as its prone towards hacking. Thus to protect this data they proposed two solutions for APKS based on a recent cryptographic primitive, Hierarchical Predicate Encryption (HPE). These are multi-dimensional keyword searches that have some queries. Thus, they enhance the query privacy that hides users’ query keywords against the server.

Manisha R. Shinde and Rahul D. Taur [6], have stated in their paper that Cloud provides a solution for daily computing related matters. Cloud Computing refers to a network that acts as a platform for deploying applications at the same time it acts as a storage server and also it provides resource on demand. The data that we are storing and working on is at high risk in terms of data hacking and this is the disadvantage of cloud computing. The authors of this paper have stated a new method for encrypting the data that are being stored in the cloud.

Aized Amin Soofi, M. Irfan Khan and Fazal-e-Amin [7], have stated that Cloud Computing is the fastest grown technology where resources and services can be got on demand. Simultaneously, this technology is gaining a lot of security issues in terms of storing the data. Data security is a big issue in cloud computing. Thus, in this paper they have done a detailed study of the encryption methods.

Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy [8], have talked about Cloud Computing and the services offered by it. They also talked about the different types of cloud, services of cloud and talked about the cloud service providers. They also said that the cloud data is not at all secure and they have to be secured using encryption purpose. They have done a detailed comparative study about the various encryption methods.

A.Mahesh Babu, G.A. Ramachandra and M.Suresh Babu [9], have discussed in their paper that Cloud computing is growing fast and the services it offers is facilitating day to day IT related works. Cloud computing offers resources and services based on demand. Cloud computing is mostly used for the storage purpose, but the storage facility is not at all safe and is prone to hacking. The data stored can be compromised and modified or loss. So, to protect this, authors have proposed a security mechanism for protecting and encrypting the data. Their idea is combining Cryptography and steganography together such that the data is safely stored and cannot be accessed by outsiders other than the sender and receiver.

Geethu Thomas, Prem Jose V and P.Afsar [10], have stated in their paper that Cloud Computing is the most trending architecture of IT industry. Cloud Computing offers various services based on different demands. It also offers storage services, but this storage service is not safe because the data can be hacked thus leading to the problem of data loss and modifiability. So the authors stated that the data that are to be uploaded in the cloud server can be encrypted using cryptography and thus can be safely stored in the cloud server.

Maha TEBAA and Said EL HAJII [11], have stated in their paper in that cloud offers various software and hardware resources. They have talked about the services that be got on-demand and can be got for lifetime by paying a minimum amount. Internet is base for cloud computing. They also said that in cloud data can be stored instead of personal hardware, but the data stored in cloud can easily compromised and stolen so to protect it they have proposed a method called homomorphic encryption technique.

Nidal M. Turab, Anas Abu Taleb and Shadi R. Masadeh [12], have stated that cloud computing is a technology that connects and helps to store resources irrespective of any location. It provides software and hardware resources. It acts as an outsourcing method. They also stated that cloud computing has its own disadvantage and the authors have done a analysis of the drawbacks and security issues and challenges of cloud computing and the biggest issue in it is the data security issue and it can be solved using the encryption methods.

V.B. Kirubanand and P.Prabhu [13], have discussed about the cloud architecture. They have made a new approach in cloud computing field with mobile –fi technology using transposition and substitution cipher techniques in job scheduling.

Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem [14], have stated that cloud computing is a very useful mode that offers resources on demand. They provide and maintain data along with applications. In cloud no need to install anything or there is no need to carry any hard drive for storing. Cloud computing a flexible mode of communication, deploy and store. Clod computing has some drawbacks as well. The data stored in cloud computing can be easily accessed and can be tampered. Thus, the authors have stated a method of protecting the data and the method is called quantum cryptography. They have proposed that quantum cryptography can be used to encrypt the data stored in cloud.

Gurpreet Kaur, and Manish Mahajan [15], have stated that cloud computing is the next big thing of the IT world. In cloud computing we can do several IT related works like storing, hosting, deploying, developing, and many more. Cloud computing is flexible, efficient and cost effective. It offers a huge storage for the users. It offers software and hardware resources. It has centralized databases, but these databases are not secured. The data stored can only be secured by using cryptography. Thus, authors have stated this and have discussed about various cryptographic techniques.

3. Existing methodologies

There are several algorithms for encryption purpose and these are being used in cloud data encryption. Listed below are some of the algorithms that are being used in our work:

a) Rail-fence cipher
b) Play-fair cipher

a) Rail-fence cipher: This is the oldest encryption technique. It is one of the symmetric encryption algorithms. The plain textual data will be encrypted using the key. The key here is the no. of rails and by following this no. the plain text is written vertically but in a zigzag pattern. The cipher text can be got if we read the message along in a horizontal way. The cipher text can be decrypted if we place the cipher text as it is in a horizontal way following the no. of rails and then read the message along the diagonal way.

The following example will describe the working of this:

E.g. **For encryption,**
Plain-text = Megha, Key or no. of rails = 2
Therefore
m………g………a…….
……e………h……….

Cipher-text = mgaeh
For decryption,
…m……g…….a..
………e……h…….

Plain-text = megha

b) Play-fair cipher: This is also one of the symmetric encryption techniques. Here, the plain text is being encrypted with the help of a key. This key also a random word. This key is then used to generate the 5*5 matrix. The plain text must be grouped.

There are certain rules for encryption and the rules are:

i) If both the elements of the pair are in same row, then they will be assigned with the next immediate element in that row in the matrix.
ii) If both the elements of the pair are in same column then they will be assigned with the below immediate element of that column in the matrix.
iii) If both the elements of the pair are in different rows or columns, then they will be assigned with the element in the corner of that same row or same column in the matrix.

There are certain rules for decryption and the rules are:

i) If both the elements of the pair are in same row, then they will be assigned with the previous located element of that row in the matrix.
ii) If both the elements of the pair are in same column then they will be assigned with the above located element of that column in the matrix.
iii) If both the elements of the pair are in different rows or columns, then they will be assigned with the element in the corner of that same row or same column in the matrix.

The following example will explain about the working of this:

E.g. For encryption,

Plain text = ANITHA= AN IT HA (Grouped)

Key = Play fair

3	L	A	Y	F
I	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Cipher-text is AN = PQ, IT = DN and
HA=QB
Therefore, PQDNQB
For decryption,

Cipher-text=PQDNQB

=PQ DN QB (Grouped)

Key = Play fair

P	L	A	Y	F
I	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Plain-text is PQ = AN
DN = IT
QB = HA
Therefore, ANITHA

4. Proposed work

Here we are showing what work we exactly proposed. Firstly, we will be showing the basic steps of our algorithm, followed by the block diagram and finally the detailed description of our algorithm. We will also be presenting the java code that will be showing the working of the algorithm.

4.1. Steps for encryption

i) Client will select their cloud service provider and will subscribe in it by creating their own account
ii) Client will select the option provided by the cloud service provider for storing various documents
iii) Client will select the data that is to be uploaded in the public cloud server
iv) The cloud server will be doing certain steps to transform the original data to cipher form before uploading it into the server.
Following are the detailed steps for encryption:
a) The server will be performing 1st stage encryption by applying Rail-fence cipher
b) 1st stage cipher text is obtained and send for 2nd stage encryption
c) Then the 2nd stage encryption is being done using the Play-fair cipher
d) Then the 2nd stage cipher text is obtained and is send for the uploading into the cloud server
v) Finally, the data is encrypted and uploaded into the public cloud server
vi)

4.2. Block diagram for encryption

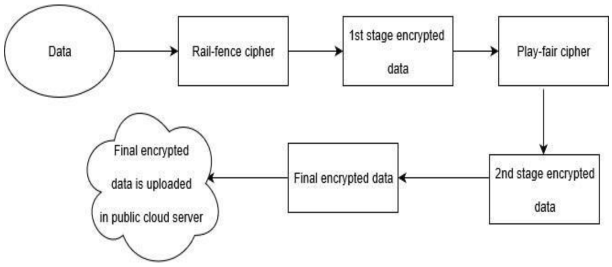


Fig. 1: Block Diagram for Encryption.

4.3. Steps for decryption

i) Client will go back to their account that they have opened under their preferred cloud service provider
ii) Client will select the encrypted data that is to be downloaded from the public cloud server
iii) The cloud server will be performing the following steps for decryption of the encrypted data:
a) The server will be performing 1st stage decryption for the Play-fair cipher
b) Then the 1st stage decrypted data is obtained
c) Then the 2nd stage decryption process is being done for the Rail-fence cipher
d) Finally, the data is decrypted, and the original text is achieved
e) Thus, the encrypted data will be decrypted finally, and the client will be able to download the file

4.4. Block diagram for decryption

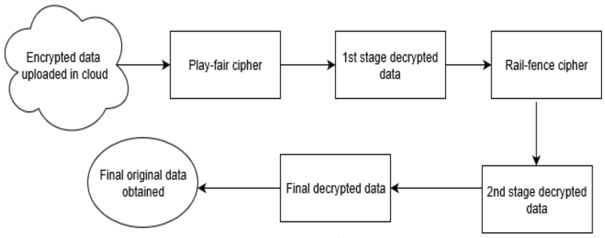


Fig. 2: Block Diagram for Decryption.

4.5. Working of our multi-phase encryption model

In this section we will be explaining the working process of our model. The following example will be having the encryption and decryption process of our model:
E.g. **For Encryption:**
1st stage encryption using Rail-fence cipher:

Plain text = RINA

No. of rails = 2

Therefore,

…R………N……….
………I…………A…….

1st stage cipher text = RNIA

2nd stage encryption using Play-fair cipher:

Previous 1st stage cipher text will act the plain text for this method = RNIA= RN IA (Grouped)

Key = Play-fair
Therefore,

P	L	A	Y	F
I	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

2nd stage or final cipher text = RN will be IO
IA will be BP
Therefore, **final cipher text = IOBP**

For Decryption:
1st stage decryption using Play-fair cipher:

cipher text = IOBP = IO BP (Grouped)

Key = Play-fair

Therefore,

P	L	A	Y	F
I	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

2nd stage or final cipher text = IO will be RN
BP will be IA
Therefore, 1st stage decrypted text = RNIA

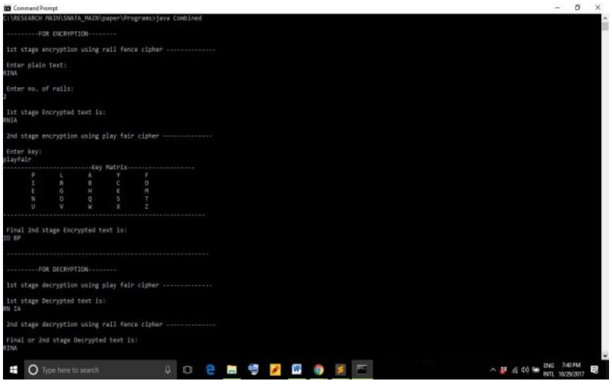
2nd stage decryption using Rail-fence cipher:
Pre-obtained 1st stage plain text is the cipher text for this method = RNIA
No. of rails = 2
Therefore, (read diagonally)

…R…………N……….
………I…………A…….

Final decrypted original text = RINA

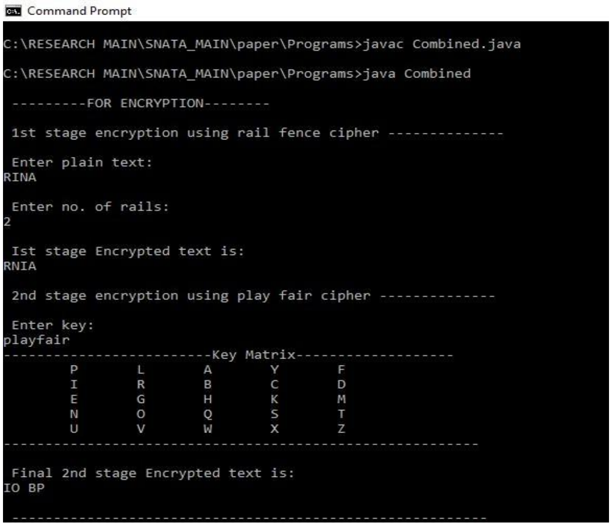
5. Result and outcomes

In this section we have shown the implementation of our work using Java language. Thus, through the implementation we have come up with an idea is that our proposed model is working with full efficiency and no errors are being caught. Following are the screenshots of our output received:



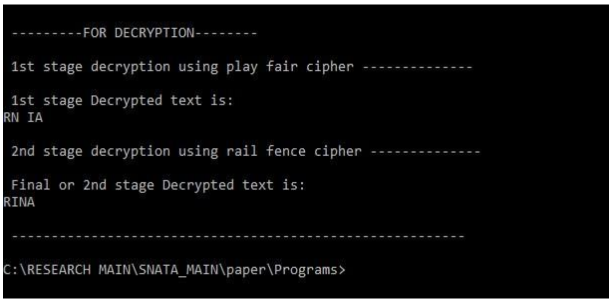
```
C:\RESEARCH MAIN\SNATA_MAIN\paper\Programs>java Combined

 ---------FOR ENCRYPTION--------

 1st stage encryption using rail fence cipher -------------

 Enter plain text:
RINA

 Enter no. of rails:
2

 Ist stage Encrypted text is:
RNIA

 2nd stage encryption using play fair cipher -------------

 Enter key:
playfair
------------------------Key Matrix------------------
        P       L       A       Y       F
        I       R       B       C       D
        E       G       H       K       M
        N       O       Q       S       T
        U       V       W       X       Z
---------------------------------------------------------

 Final 2nd stage Encrypted text is:
IO BP

 --------------------------------------------------------

 ---------FOR DECRYPTION--------

 1st stage decryption using play fair cipher -------------

 1st stage Decrypted text is:
RN IA

 2nd stage decryption using rail fence cipher -------------

 Final or 2nd stage Decrypted text is:
RINA
```

Fig. 3: Java Implementation of Our Algorithm.



```
C:\RESEARCH MAIN\SNATA_MAIN\paper\Programs>javac Combined.java

C:\RESEARCH MAIN\SNATA_MAIN\paper\Programs>java Combined

 ---------FOR ENCRYPTION--------

 1st stage encryption using rail fence cipher -------------

 Enter plain text:
RINA

 Enter no. of rails:
2

 Ist stage Encrypted text is:
RNIA

 2nd stage encryption using play fair cipher -------------

 Enter key:
playfair
------------------------Key Matrix-------------------
        P       L       A       Y       F
        I       R       B       C       D
        E       G       H       K       M
        N       O       Q       S       T
        U       V       W       X       Z
-------------------------------------------------------

 Final 2nd stage Encrypted text is:
IO BP

 ------------------------------------------------------
```

Fig. 4: Encryption Phase of Our Algorithm.



```
 ---------FOR DECRYPTION--------

 1st stage decryption using play fair cipher -------------

 1st stage Decrypted text is:
RN IA

 2nd stage decryption using rail fence cipher -------------

 Final or 2nd stage Decrypted text is:
RINA

 ------------------------------------------------------

C:\RESEARCH MAIN\SNATA_MAIN\paper\Programs>
```

Fig. 5: Decryption Phase of Our Algorithm.

6. Conclusion and future work

Cloud Computing is a vast application for storing data, running any application, or accessing any application. Simultaneously, the security regarding the data is also at stake due to the vulnerability of the data towards the attackers. This is because the entire cloud structure is based on the internet and there is no proper security regarding the data in cloud. This is mostly in public cloud and general users nowadays mostly use the cloud and their entire data is saved there but this public cloud is not at all safe. Thus, our research work is based on encrypting the data that is to be stored in the public cloud such that the data becomes less vulnerable towards attackers. In order to safeguard this data, we have implemented a multi-phased encryption model that is performing the encryption efficiently without any error. Our future works basically aims at the implementation of this model fully in real time and modify it more based on real time demands.

Acknowledgement

This research was undertaken under the able guidance of Dr. Kirubanand V.B., Professor, Dr. Rohini V., coordinator and Dr. Joy Paulose, H.O.D, Christ University, as a part of Computer Science Department.

References

[1] Shakeeba S. Khan, Prof. R. R. Tuteja, K., ”Security in Cloud Computing using Cryptographic Algorithms”, International Journal of Innovative Research in Computer and Communication, Vol. 3, Issue 1, January 2015.

[2] P. Subhasri, Dr. A.P admapriya, “Multilevel Encryption for Ensuring Public Cloud”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 7, July 2013.

[3] Karun Handa, Uma Singh, “ Data Security in Cloud Computing using Encryption and Steganography “, International Journal of Computer Science and Mobile Computing, Vol. 4, Issue 5, May 2015.

[4] Treesa Maria Vincent, Mrs. J Sakunthala, “Encrypted Data Storage in Cloud Environment”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 3, March 2013.

[5] Ming Li, Shucheng Yu, Ning Cao and Wenjing Lou, “Authorized Private Keyword Search over Encrypted Data in Cloud Computing”, 31st International Conference on Distributed Computing Systems, 2011. https://doi.org/10.1109/ICDCS.2011.55.

[6] Manisha R. Shinde and Rahul D. Taur,” Encryption Algorithm for Data Security and Privacy in Cloud Storage”, AJCSES [3] [1] [2015] 034-039.

[7] Aized Aim Soofi, M.Irfan Khan and fazal-e-Amin, “ Encryption Techniques for Data Confidentiality”, International Journal of Grid Distribution Computing, Vol. 7, No.4,2014

[8] Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy, “Cloud Computing: Security Issues and Research Challenges”, International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[9] A. Mahesh Babu, G.A. Ramachandra, M.Suresh Babu, “Implementation of Security in Cloud Systems Based using Encryption and Steganography “, International Journal of Electrical, Electronics and Computer Systems (IJEECS), ISSN (Online): 2347-2820, Volume - 3, Issue-11 2015.

[10] Geethu Thomas, Prem Jose V and P.Afsar,”Cloud computing security using encryption technique”.

[11] Maha TEBAA, Said EL HAJII, “Secure Cloud Computing through Homomorphic Encryption”, International Journal of Advancements in Computing Technology (IJACT) Volume5, Number16, December 2013.

[12] Nidal M. Turab, Anas Abu Taleb Shadi R. Masadeh,” Cloud Computing Challenges and Solutions”, International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.5, September 2013.

[13] V.B Kirubanad, P.Prabu, “Cloud Computing with Mobile-Fi Technology using transposition and substitution cipher in Job Scheduling.

[14] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, “Cloud Computing Cryptography "State-of-theArt", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:7, No:8, 2013.

[15] Gurpreet Kaur, Manish Mahajan, “Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms”, Int. Journal of Engineering Research and Applications, Vol. 3, Issue 5, Sep-Oct 2013, pp.782-786.