e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

An Approach to develop Encryption Algorithm to enhance Data Security in private cloud computing

Vishal K Upadhyay[1], Dr. Vinod L Desai[2]
[1] *DCS, Research Scholar Mewar University Chhittogarh (Rajasthan),*
[2] *Govt. Science College, Chikhali (B.Sc.Computer Science Dept.)*

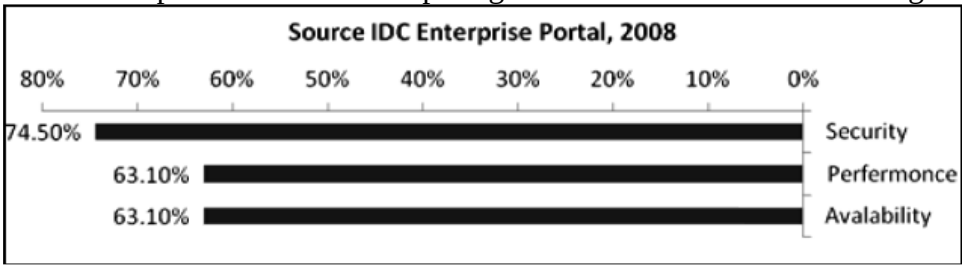
Abstract – The cloud computing in present time is appreciated to offers unbound storage capacity, effective data storage management but have some concern about data securities. This paper presented the basic information about the cloud computing and its security condenses. Furtherance in the paper has attempted to improve the security in private cloud computing by offering an encryption algorithm.
Keywords: Private Cloud Computing, Data Security, Encryption Algorithm

I. INTRODUCTION

The secure and private data stored in the network are the main obstacles in the area of computerization. Security and privacy are the major issues in storage across the cloud. This paper suggests the encryption algorithm to address the security of privacy in the cloud storage to protect stored data. Cloud Computing provides computer resources (servers, storage, operating system) to the user on request. Cloud computing solution has emerged popular and provides easy access to the outsourcing of information technology and resources. An increasing number of agencies take advantage of cloud computing applications to host [1]– [2]. Virtualization Support basic concept of cloud computing. Resources are provided to cloud users as virtualized manner[3]. Computing, virtualization can be used successfully to improve flexible computing environment. It provides the means to retrieve components or the system using the failover. Quickly take backup application data task. Virtual machines can be migrated from one physical server to another district in migration; default images can be re-run in a different location [4].

A cloud computing has different three types of services. Software as a service (SaaS), Platform as a service(PaaS) and Infrastructure as a service(IaaS). Cloud computing services are provided by providers of different cloud such as Amazon Google, Microsoft, IBM, etc. Users can use these services (Saas PaaS, IaaS) according to the uses. The service provider of different cloud environment now preserving the user data. Cloud Computing with all users "data are stored on the Cloud". So users to think about the data[5]: data security in the Cloud, access control, and Cloud authentication. Cloud Computing Companies says that your data is safe, but it is too primary to say. Only time will tell if the user's data is secure in cloud database.

Cloud Computing security is born in which customer data request from suppliers who reside in the workplace. Security have always been a major concern in cloud computing [6]– [7] as shown in Fig.1. Study shows the report of 2008 and 2009 from International Data Corporation. In the figure, it is clear that security is the most important in cloud computing in the framework of the investigation two years.



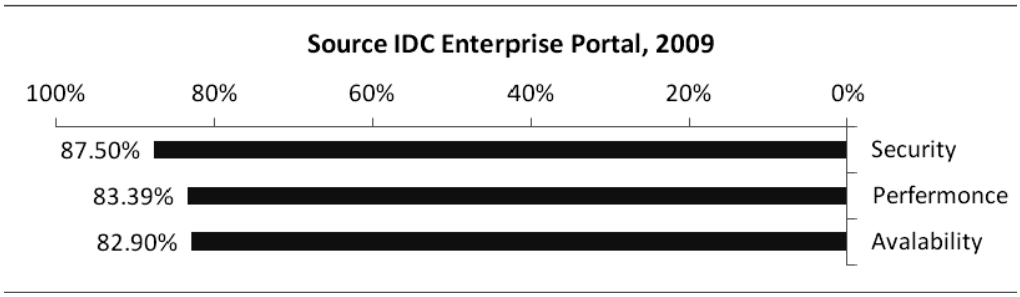


Figure 1 security is a major concern for cloud computing [6] – [7]

The costs and easiness of use are the benefits of cloud computing [5], there are important security problems that must be addressed, while the important applications and sensitive data, storage in to the private cloud computing.

In the cloud computing there can be a two different type of attacks. One is Insider and Second is Outsider attacks. Insider as an administrator may have the capacity to penetrate the user data. Internal Attack very difficult to identify. For that users should be very careful with data storage in storage across the cloud computing. Even if the data is available from a third party, not to be access to actual data. Therefore, it must be encrypted data before being transferred to the storage across the cloud computing.

Public-key cryptography is the application for encryption and decryption. In the area of encryption methods many of encryption/decryption applications available. These techniques can be broadly classified into two major groups, any classic and public-key cryptography [8]. Classic Encryption is also mentioned as encryption or single key encryption. This use of the same key in encryption and decryption. public key cryptography is referred as public-key cryptography or encryption. An independent keys used for encryption and decryption. Figure 2 represents a simplified model interactive encryption technology.

Original message understood, referred to in the text of the clear objective of transforming random ambiguous message in encrypted text. The encryption algorithm is composed of major. This is the value of specific independent of plain text. The algorithm will produce different production by user at this time. Changing the key modify output of the algorithm.

Once the encrypted text is the produced, it can be communicated to storage data across the cloud computing. During the reception, the encrypted text can be converted to clear out of encoding algorithm using the same key, which is used for encryption.

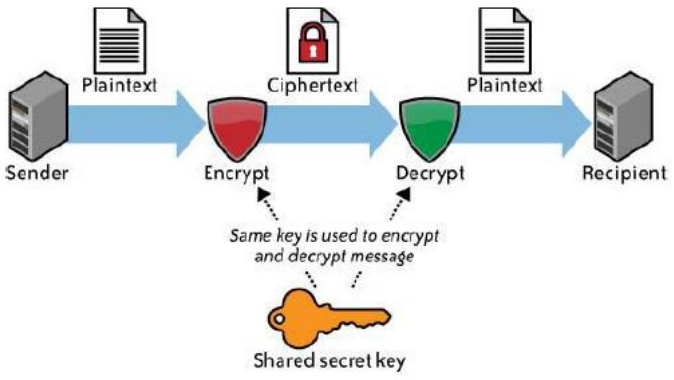


Figure 2 Model of Conventional Encryption [9]

We develop proposes encryption algorithm to protect user data stored in the cloud computing from unauthorized access.

II. PROBLEM IN CLOUD DATA STORAGE

Cloud computing Transfer applications and data to a cloud storage, where data management and services may not be completely reliable. This same feature, however, increases many new security challenges that have not been well understood we focuses on a cloud data storage of security, which has always been an important aspect of the quality of the service.

Here we discuss problems [10] of cloud data storage.

A. privacy

Different from the traditional model of computing, virtual computing technology used personal computing user data can be deployed in various virtualized data centers, instead of staying in the same site even across national borders. At this time, privacy and protection of data will face a controversy of various legal systems. Meanwhile, users can leak hidden information when access to cloud computing services. An attacker could analysis of important tasks, according to the account provided by the users. Major problems of protecting privacy [11] focus on the 1) confidence, that is to say, if it is not permitted on the personal information of secondary (personally identifiable information), and the 2) uncertainty, i.e. to ensure that the data have been disposed of in a timely manner of the person who controls the data retention on the way in which the non-obligation of confidentiality, how to determine the error in 3) compliance with, any global environments Dynamic data, the flow and deal with difficulty in compliance with the flow requirements.

B. Security

Cloud computing related security issues in risk areas such as external data storage, dependency on the public internet, and lack of control over multi-tenancy and integration of internal security [12]. The Service Providers of cloud used to store and convert data in encryption format and use authentication and authorization. Many customers are concerned about the lack of data by the hackers. The service provider of cloud computing are very sensitive to this issue they apply to many of the resources to improve this problem.

C. Confidence

The question of confidence in cloud computing has a concern on security and privacy. Assign User data to third-party services offers cloud computing on the problem. For example, in April 2012, Amazon Elastic computing cloud service crashed during the upgrade of the system. Another incident occurred in the same month. Hackers broke into a network Sony PlayStation, get personal information of 77 million people in the world. It is certain that these issues may create doubts in the minds of the cloud users and undermine trust [10].

D. Ownership

After these data are store in to the cloud, the developers were afraid of losing their rights or unable to protect the rights of their clients. Many cloud providers address this issue with well-skilled user-sided agreements. According to the agreement, the users will be wise to seek the opinion of your preferred legal representative.

E. Performance and Availability

Companies on the acceptable levels of performance and availability of applications that are hosted by the cloud computing. The application of the data in the storage across the cloud network should be available to users at any time and in any place. The users have no reason to concern on the local system that uses access to cloud servers.

F. on the long term Viability

Users must ensure that the data in the network does not become invalid, so the cloud computing SUBMITTED BY lose or gain and swallowed the largest company. Users must be asked to potential

suppliers of cloud how can access to user data and whether that would be in a form that can be used to import the replacement request [13].

H. Data Backup

The Service Providers of could computing servers use periodic backup data backup process, but concern about the ability to control the backup operations. Many providers are now offering data dumps onto media or allowing users to back up data through regular downloads.

G. Data conversion Mobility

Data users fears of mobility, to switch between the providers of services. It may be difficult to transfer data. Portage and conversion of data depending on the nature of the cloud service provider in the form of data retrieval, especially in cases where the form can be easily. The evolution of competition, the open standards have become data and scalability The issue of facilitating transfer operations available to support service providers of networks of people. In the worst cases, it was noted that the cloud participants to pay in an ad hoc manner to transfer data. These are some of the areas of computing in the clouds the need to Excel, and the solution of problems related to this problem. Of all these problems, the safety and protection of private data[14] main threats to the growth of cloud computing . It needs to work.

III. ENCRYPTION

Encryption (see figure 2) use the secret key to encrypt and decrypt data. Encryption only speedy and efficiency to manage large quantities of data encryption [9].

For example, a source sends clear message $X = (X_1, X_2, X_3,... X_M)$. Encryption key on the source of the message. And then also to the destination via secure channel. With the letter X Encryption Key K as input, the encryption algorithm encrypted text $Y = (Y_1, Y_2, ...,Y_N)$. This can be writing $Y = E_K(X)$. Encrypted text Y resulting from the use of encryption algorithm or refers to the Encryption algorithm used K determines the key is used for encryption. The beneficiary of this letter that the application of the algorithm decrypt with the same key is used for encryption to get the true message $X = D_K [Y]$. Here D refers to the decryption algorithm.

IV. CLASSIC ENCRYPTION

Several encryption algorithms available, which are used in the field of information security. The encryption algorithms can be classified as classic [15]. Encryption algorithms this is based on the general principles is replacement of blades in each element in plain text to another element, and encryption by quotation in elements in plain text is organizing. Encryption algorithms some different algorithms in this section.

A. Caesar Cipher

Caesar Cipher [16] is a classical substitution cipher and it is one of the simplest examples of substitution cipher. It replaces the character of the letter in plain text, with letter 3 places. For example, "WORLD" is the text that will be converted to "MOORE" in encrypted text. We can see that such codes may be difficult to break. This could be the break the encryption of the brutal attack, because in the end there are only 25 possible options available.

B. Playfair cipher

Another example of replacing cipher is Playfair cipher encryption [17] which has a matrix square 5X5 according to the alphabetical order messages appropriate manner. The user can select a key in the array. Letters of the alphabet of the switch, and then one after the other in a matrix Playfair Cipher. The plain text is broken into pairs and if a pair has same alphabet then they are separated by introducing a filler letter with ‘x’. Otherwise if the pair is with different alphabetical letters and resides in the same row of

matrix then each letter is replaced by the letter ahead of it. If the pair of letters is in same column of matrix then each letter is replaced by the letter below it, and when the pair of letters is neither in same column nor in same row then they are replaced by the letter in their row that resides at the intersection of paired letters.

C. Vigenere Cipher

Vigenere Cipher [18] when compared with Caesar cipher gives some level of security with the key word. This word is repeated along the plain text needs to be encrypted. For example below:

KEY: a x c m z o y n p e j b

Plain text: c r y p t o g r a p h y

Cipher (Encryption): J Q X J U A M F S N P S

As is clear from the above example, " a x c m z o y n p e j b " is the key word and plain text " c r y p t o g r a p h y " which has been encrypted in " J Q X J U A M F S N P S ". This is done using vigenere table containing alphabets in the form of rows and columns the column to the left. In the far left column keyword, which is the highest rank in the clear in the intersection between letters of the alphabet is the alternative. After processing each message individually, user receives an encrypted message.

D. Rail fence technique

This is one of the encryption application [8], in the written text in the form of a series of Diagonal then read about a series of lines . For example, to encrypt the message "hello world" with rail fence of depth 2.

h e l w l r o

o d l w

Encrypted Message now is " helwlroodlw".

In the same method in plain text basics of the reorganization. This method may not be sufficient to ensure the security of the data.

V. PROPOSED ALGORITHM

Proposed technical focus on improving encryption techniques in classical encryption. The replacement borrowing methods of using the alphabet to encrypt the text. In the algorithm proposed, in the first time is transforming plain text to the corresponding to the value of the ASCII code of all the alphabet. Classic encryption technology in the key value from 1 to 26 or keys can be a series (Group of alphabets). But in the main algorithm proposed a value between 1 and 256. This algorithm is used to encrypt user data in cloud computing. Because the user has no control over the data after the session encryption key major work of user authentication. The algorithm proposed set out below.

A. Encryption Algorithm

Here encryption algorithm steps…

Encryption Algorithm:

Step 1. Calculate the number of characters (n) In the text without space.

Step 2. Transforming plain text to the equivalent of ASCII code. and the form of a matrix Square ($S \times S >= N$).

Step 3. The application of the currency ASCII code for the value of the left-to-right in the matix. Matrix divided into three parts of knowledge to the upper triangle, lower triangle and crosswise.

Step 4. Read the value of the right to the left of each matrix.

Step 5. Use all three different main matrix $K=k_1$, K_2 K_3 encryption. Then Do encryption.

Step 6. Encryption application value in the matrix on the same upper and lower triangle.

Step 7. Read the message of the column of the columns. Here in the columns of the Matrix is the key K_4.

Step 8. Convert the ASCII (American Standard Code for Information Interchange) code into character value.

Here a detailed description of each step in the proposed encryption algorithm.

Step 1:- Calculate the No. characters (n) In a letter without space.
Plain Text. HELLOWORLDU.
N = 11 (N = the number of characters in the message)
Step 2: Convert plain text to the equivalent of ASCII code. And form a Square matrix.

ASCII code for the value of the Plain Text:
72 73 72 79 87 65 82 69 89 79 85
To form a square matrix, choose a number (S), square value of S is immediately next to N. i.e. S^2 is nearest square value N and $S^2 >= N$.
This clear text N = 11, so S=4.
The order of matrix is $4 \times 4 >= 11$, Form a 4×4 matrix.
Step 3:- Apply the converted ASCII code message row by row in S X S matrix. Separate the matrix into three parts as Upper, Lower triangle. Following shapes represent the upper, crosswise and lower triangle position in the square matrix.
Upper triangle, lower triangle and crosswise.

72	73	72	79
87	65	82	69
89	79	85	65
66	67	68	69

Step 4: Read the letter from left to right at the upper triangle crosswise and lower triangle.

72	73	72	79
87	65	82	69
89	79	85	65
66	67	68	69

Values of three triangle are.
Upper Triangle 73 72 79 82 69 65
crosswise 72 65 85 69
Lower Triangle 87 89 79 66 67 68
Step 5: To encrypt the message using three different key at upper triangle, crosswise and lower triangle separately. Keys are $K=K_1$ upper triangle, K_2 for crosswise and K_3 for the lower triangle.
Upper Triangle = 23 - K1
crosswise =17 K2
Lower Triangle = 6 - K3
Now add this key value with ASCII code for a message every matrix.
After encryption:
Upper Triangle 95 102 105 92 96 88
crosswise 89 82 102 89 86

Lower Triangle 93 95 85 72 73 74
Step 6: apply in a matrix square in the same way.

89	96	95	102
93	82	105	92
95	85	102	88
72	73	74	86

Step 7: now read the message of the matrix column by columns. Here the order of the columns read in the matrix is the key K_4.

4 2 1 3 Key- K_4

89	96	95	102
93	82	105	92
95	85	102	88
72	73	74	86

Encrypted text is:
95 105 102 74 96 82 85 73 102 92 88 86 89 93 95 72
Step 8: Convert the ASCII character code into equivalent value. Then,
Encrypted cipher text _ifj.ruif\xvy]_h

B. Decryption Algorithm

Encrypt data stored in storage across the cloud. Retrieving data from the cloud, the decoder must have access to data in the cloud. On the decoder only with the values that use encryption. We must therefore have a vital role in encryption and decryption algorithm. The following steps for decryption algorithm.

Decryption Algorithm:

Step 1. Encrypted text are converted in to the ASCII code values.
Step 2. Count the No. of character (N) in the decrypted text and form a square matrix S $_X$ S.
Step 3.Then apply the ASCII code in the matrix of SXS as column by column based on key K_4.
Step 4. Dividing the matrix in upper triangle, crosswise, and lower triangle.
Step 5. Apply reverse encryption using the keys K_1, K_2 and K_3 on the upper triangle, crosswise and lower triangle respectively.
Step 6. Apply the message into table by upper triangle, crosswise and lower triangle.
Step 7. Read the message as row by row from left to right.
Step 8 .Convert code ASCII (American Standard Code for Information Interchange) in the value of the character.

Here a detailed description of each step in the decryption algorithm.
Step 1: Each character in encrypted text to the equivalent of ASCII code values.
Encrypted text = _ifj.ruif\xvy]_h

Converted to ASCII code, as shown below
95 105 102 74 96 82 85 73 102 92 88 86 89 93 95 72

Step 2:- Calculate the Number of characters (N) to decode the text matrix square S_XS.
Number of characters N = 16, S=4, of the matrix is 4_X4.
Step 3: Use ASCII code in the matrix SxS on a column by column base on key K_4.
Now in the matrix is,

4 2 1 3 Key- K_4

89	96	95	102
93	82	105	92
95	85	102	88
72	73	74	86

step4:- Dividing the matrix in upper triangle, crosswise and lower triangle.
Read the message in the matrices from the left to the right.

89	96	95	102
93	82	105	92
95	85	102	88
72	73	74	86

Now, all the matrix
Upper Triangle 96 95 102 105 92 88
Crosswise 89 82 102 86
Lower Triangle 93 95 85 72 73 74

step5:- Then use the reverse the encryption keys using K_1 K_2 and K_3 on the upper triangle, crosswise and lower triangle.
Upper Triangle = 23 - K_1
Crosswise =17- K_2
Lower Triangle = 6 - K_3

Decrypt the message using the keyboard. Three matrixes values after the decoder
Upper Triangle 73 72 79 82 69 65
Crosswise 72 65 85 69
Lower Triangle 87 89 79 66 67 68

Step6:- Then apply the message into table by upper triangle, Crosswise and Lower Triangle.

The matrix is,

72	73	72	79
87	65	82	69
89	79	85	65
66	67	68	69

step7:- Read the message as row by row from left to right.

72	73	72	79
87	65	82	69
89	79	85	65
66	67	68	69

Now, a message,
72 73 72 79 87 65 82 69 89 79 85 65 66 67 68 69
Step8:- Convert ASCII code characters in to the equal character value. And then, decryption result is.

HELLOWORLDU

The work of all these steps the algorithm to decrypt the original text retrieval is used. The encryption and decryption key and the more important.

VI. CONCLUSION

The security of data stored in the private cloud computing space are full of challenges. Till many problems have not been identified. Cryptographic techniques used to ensure contact between the user and cloud. Encryption fast and efficient management of large amounts of data storage across the network. This document proposes the encryption algorithm to ensure user data of cloud storage cloud. Encryption algorithm is described in detail, in the process of the decoder is to reverse the encryption. This algorithm is used to encrypt data used in the network. Because the user has no control over the data once the separation of the encryption key of user authentication. The application of this encryption algorithm is used to ensure that the data stored on the safe storage and cannot be accessed from officials or outsider.

REFERENCE

[1] J. Srinivas, K. Vemireddi Venkata Reddy subba Dr moiz qyser A, "Fundamentals of cloud computing", International Journal advanced research in the field of informatics and communications engineering vol.1 number 5, pp. 343 -347, 2012.

[2] chunye Gong J Liu Qiang, Zhang Haitao Chen henghu Gong, "characteristics of cloud computing ", 39 international conference on parallel processing workshops, IEEE xplore, 1530 - 2016/10, para. 275 -279, 2010.

[3] Karen scarfone, murugiah souppaya Paul Hoffman guide to security for full virtualization technologies,http://csrc.nist.gov/publications/nistpubs/800-125/sp800-125-Another.pdf, abbreviated NIST, 2011.

[4] Stratus technologies, White Paper on Server Virtualization cloudcomputing: Four effects hidden at the time of work and ± "http://www.stratus.com/~/media/stratus/files/library/whitepapers/servervirtualizationandcloudcomputing.pdf, 2011.

[5] Eman Mr. Mohammad Hatem S. Abdul Qader and Mayor el-etriby, computing data security model ,Twelfth International Conference on networks ISBN: 978-1 -61208-245-5, paragraph 66-74, 2013.

[6] Peter mell Tim Grance effectiveness and safety of using cloud computing model, abbreviated NIST information technology laboratory http://www.csrc.nist.gov/groups/sns/cloud-comput G/cloudcomputing. v26. 2009 PPT.

[7] Frank Gens et al, cloud computing on the International Data Center (IDC) 2010 http://www.cionet.com/data/files/groups/cloud%20computing%2 02010 20% TO 20% % % International Data Center (IDC) 20 20 update.pdf, 2010.

[8] William stallings, encryption and Network Security: principles and practices Bohemia, fifth edition, Prentice Hall ISBN 13: 978 A. -0136097044, 2010.

[9] Tim Mather, Subra Kumaraswamy, and Shahed Latif cloud security and confidentiality A. Reilly Media , Inc. , 61 - 71, 2009.

[10] Mohit marwaha, rajeev Bedi use of the encryption algorithm for the security and confidentiality of data in computing ijcsi International Journal computer science, vol. 10, 1, 1, para. 367 -370, 2013.

[11] Siani Pearson privacy, security and trust in cloud computing, HP laboratories, hpl-2012-80r1, has appeared in a book chapter of Springer, paragraph 1-56, 2012.

[12] K hashizume et al, analysis of security issues cloud computing, magazine, Internet services and applications open Springer party newspaper 1-13, 2013.

[13] Pankaj Arora et al., cloud computing security issues in infrastructure as a service, International Journal Advanced Research in Computer Science and Software Engineering, vol. 2, No. 1, 2012.

[14] pardeep Sharma, Sandeep K. Sud, and Summet kaur, security issues in computing, Springer Verlag Berlin Heidelberg, HPAGC 2011 169 Chambers of Commerce and Industry, 36.45, 2011.

[15] vamsee Krishna Yarlagadda and sriram ramanujam, data security in computing , Journal of Computer Sciences and Mathematics vol. 2 (1), pp. 15 -23, 2011.

16] Dr. A. padmapriya , p subhasri, cloud computing: Reversing the encryption algorithm Caesar to increase data security, International Journal engineering and technology trends - Volume 4 inserted4, 1067-1071, 2013.

[17] V.U.K. Sastry, N. Ravi Shankar and S. Durga Bhavani, circulated degree Emma Playfair encryption intermarriage, and iterative process nesting of, International Journal of the mobile network, and technologies, pp 45-53, 2010.

[18] quist-aphetsi kester Hybrid Cryptosystem Based on vigenere code transfer Bohemia, International Journal of advanced technology and engineering research (ijater), vol. 3, No. 1, para. 141 -147, 2013.

