ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

Efficient Cryptography Technique for Data Security using Binary Tree

A Vanaja

Lecturer, Dept. of Computer Science and Applications, St Aloysius College(Autonomous), Mangalore, Karnataka, India.

ABSTRACT: It's an era of cloud computing. It is a growing technology. It provides massive capacity of storage for cloud users. Cloud storage is more flexible as a function of user's to store and retrieve their data as their requirement. So it's necessary to protect the data transmitted over the different servers. Cloud allows users to use without installation and access their personal data at any computer with internet access. It is known that,As technology increases the security issues also increases which happened also in cloud computing. Such a way the major issues on the cloud computing are data privacy and security.This paper has proposed Encryption algorithm to meet the security and privacy issues in cloud warehouse in order to protect the data stored in the cloud.

KEYWORDS: Cloud computing, Cloud storage, Cloud warehouse, Security, Privacy, Encryption Algorithm, Cryptography.

I. INTRODUCTION

Cloud computing is an emerging technology in this world. It provides the services to the users based on their demand. Cloud computing is a common independent remote servers to support data and applications [1]. Cloud has three different services such as software, Platform, Infrastructure. Cloud services are provided by the different cloud providers like Amazon, Google, Apple, IBM and etc. User can utilize these services depends on the need[2]. "It can be challenging to get large enterprises to trust the cloud, so this partnership with Vormetric provides a significant security measure required to overcome that concern," says Pete Nicoletti, director of security and compliance at Virtustream. "It is important to utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility," says Tumulak. He says that an effective cloud security solution should incorporate three key capabilities[3].

1. Data lockdown
2. Access policies
3. Security intelligence
4.

Data lockdown-make sure that data is not readable and that the solution offers strong key management. Access policies- implement access policies that ensure only authorized users can gain access to sensitive information. Security intelligence- incorporate security intelligence that generates log information, which can be used for behavioral analysis to provide alerts that trigger when users are performing actions outside of the norm. "It can be challenging to get large enterprises to trust the cloud, so this partnership with Vormetric provides a significant security measure required to overcome that concern," says Pete Nicoletti, director of security and compliance at Virtustream[3].

The main aim of this paper is the new way of data security solution with encryption, Which can be used as a reference for designing the complete security solution.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

II. CLOUD COMPUTING CHALLENGES

In cloud computing security is an essential service to protect the data. It ensures to enhance the business performance. Cloud service provider makes sure that customers should get uninterrupted service with losing any data and with the originality [5].When we discuss about security there are five types of issues arise:

1. Data Authentication Issues.
2. Data Privacy Issues.
3. Traditional Security Issues.
4. Infected Application.
5. Accessibility Issues.
6. Securing Data Storage
7.

1. Data Authentication Issues:

The data on the cloud is common, private, sensitive data. It can be accessed by anyone at anytime from anywhere. So it is possible any cloud computing service provider and consumer can modify the data. The common problem in cloud computing is data theft and data leaking.

2. Data Privacy Issues:

A strong monitor is require to hold data privacy. Like the cloud service provider should make sure that who is accessing the data and who is managing the data so that the service provider can protect the data.

3. Traditional security issues:

Cloud computing security must be done. It may have to go different levels in provider side as well as user side. so that we can overcome the problem of data stealing, data loose, data leaking.

4. Infected Application:

Any malicious user from uploading any infected application onto the cloud which will severly affect the customer and cloud computing service.

5.Accessability Issues:

Cloud providers assure customers that will have uninterrupted predictable access to their data.

6.Securing data storage :

Here main concern is to protecting data for unauthorized users

III . TECHNIQUES FOR PROTECTING DATA IN THE CLOUD

Traditional models of data protection have often focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems. But this approach does not provide sufficient protection against APTs, privileged users, or other insidious types of security attacks While many organizations have implemented encryption for data security. In this scheme encryption keys must be sufficiently protected. The encryption implementation must incorporate a robust key management solution to provide assurance that the keys are sufficiently protected. It's critical to audit the entire encryption and key management solution. Encryption works in concert with other core data security technologies, gleaning increased security intelligence, to provide a comprehensive multilayered approach to protecting sensitive data and mitigate risk in or out of the cloud. In this paper we are proposing a new encryption scheme for secure data storage on cloud

IV . PROPOSED ALGORITHM FOR DATA ENCRYPTION

ENCRYPTION ALGORITHM

Step 1: Count the No. of character (N) in the plain text
without space.

Step 2:Convert the plain text into equivalent ASCII code.

Step 3: Find out the difference between the ASCII code such as

V1 V2 V3 V4 V5 …..

L1: V1-V2 V2-V3 V3-V4 V4-V5……

Step 4:Take modulus for L1 elements & store it in L2

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

L2=|L1|
Like L2=|V1-V2| |V1-V2| |V1-V2| |V1-V2| |V1-V2|….
L2=X1 X2 X3 X4 X5….
Step 5:From L2 find out the greatest no and store it in G.
Step 6:From ASCII code value form a binary search tree.
Step 7:From binary search tree write Pre-order & In-order.
Step 8:To encrypt the text different keys are used in different levels They are
L1→k1=33
Pre-Order →k2=3
In-Order →k3=2
N , G → k4=32
Add k1 with L1 elements,k2 with Pre-order elements,k3 with In-order elements,k4 with N &G.

Step 9:Encryption format
Here use another key k5
K5=NGInorderPreorderL2
Use k5 to Encrypt the text.
Step 10:Convert the ASCII code into character value.

DECRYPTION ALGORITHM

The encrypted data is stored in the cloud,decryption is necessary to get the actual data in the cloud. Decryption is possible only with key values which are used for encryption. So key should have a vital role in encryption and decryption algorithm.
Step1: The encrypted text is converted into ASCII code.
Step 2: Extract 1st&2nd ASCII code and apply reverse encryption using k4 & store in N,G respectively .
Step 3: From the ASCII code message extract the ASCII code from 3rd positionupto N elements. Then apply reverse encryption using key k3 and store it in I.
Step 4: From the ASCII code message extract the ASCII code from N+3rd position up to N elements. Then apply reverse encryption using key k3 and store it in P.
Step 5: Construct a binary search tree using I & P.
Step 6:Write pre-order & store it an array A.
Step 7: With the remaining code message apply reverse encryption using the key k1.
Then apply the following formula with each ASCII code find out X value.
G-ASCII code=X
Find out X value for all ASCII Code & store it an array B.
Step 8: Using the following algorithm rearrange array A elements such a way the difference of
A[0], A[1] should be B[0] &
A[1], A[2] should be B[1] &
A[2], A[3] should be B[2] such as ..

```
Count=0,flag=1
Do{
        for(i=0,j=1;i<=j+1;i++)
        {
                Flag=1
                If(A[i]-A[i+1]==B [i])
                {

                        j=i+1;
                        count=count+1;
                        flag=0;
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

```
                    }
                    If(count==N)
                            Break;
                    Else if(count>N && flag==1)
                    {
                            Temp=A[j];
                            A[j]=A[j+1];
                            A[j+1]=temp;
                            i=0;j=1;count=0;
                    }
            }
    }while(count<n);
```

Step 9: Write the array elements A(ASCII Code).
Step 10: Convert the ASCII code into equivalent character value.

By completion of all these steps in the decryption algorithm the receiver can receive the original text.

V .THEORETICAL ANALYSIS OF THE PROPOSED ALOGORITHM

The data has to be encrypted before it gets stores in cloud so that data can be protected. When customer request the from the cloud data has to be encrypted, this process is known as cryptography. This section is having the theoretical analysis of the proposed algorithm. The data which has to be encrypted is known as plain text. Count the plain text character without white space. (eg: frank,N=5)Convert the plain text into equivalent ASCII code- 102 114 97 110 107. Find out the difference between the ASCII code (L1: -2 17 -13 3) and take modulus for all elements. From that find out the greatest no and store it in G(17). From ASCII code value form a binary search tree. From binary search tree write Pre-order & In-order (Pre-order: 102 97 114 110 107 and In-order : 97 102 107 110 114).Then the text has to be encrypted for that different keys are used in different levels. They are k1=33,Pre-Order →k2=3, In-Order →k3=2 and N , G → k4=32 then add k1 with L1 elements,k2 with Pre-order elements,k3 with In-order elements,k4 with N &G. Encryption format -Here use another key k5=NGInorderPreorderL2(37 49 99 104 109 112 116 105 100 117 113 110 52 33 63 47). Convert the ASCII code into character value(%1chmptiduqn4!?/).

When the customers access the data from the cloud it will be in the form encrypted. To read the encrypted data it has to decrypted. So here decryption technology has to be applied (%1chmptiduqn4!?/). The encrypted text has to be converted into ASCII code(37 49 99 104 109 112 116 105 100 117 113 110 52 33 63 47). Extract 1st &2nd ASCII code and apply reverse encryption using k4 and store in N,G respectively(5,17) . From the ASCII code message extract the ASCII code from 3rd position up to N elements. Then apply reverse encryption using key k3 and store it in I(I: 97 102 107 110 114). From the ASCII code message extract the ASCII code from N+3rd position up to N elements. Then apply reverse encryption using key k3 and store it in P(P: 102 97 114 110 107). Construct a binary search tree using I & P. Write pre-order & store it an array A(102 97 114 110 107). With the remaining code message apply reverse encryption using the key k1(52 33 63 47). Then apply the following formula with each ASCII code find out X value.

G-ASCII code=X

And find out X value for all ASCII Code & store it an array B. Using the following algorithm rearrange array A elements such a way the difference of(-2 17 -13 3)

A[0], A[1] should be B[0] &
A[1], A[2] should be B[1] &
A[2], A[3] should be B[2] such as ..

Then write the array elements A (ASCII Code:102 114 97 110 107). Then convert the ASCII code into equivalent character value(frank). This will be plain text.
The following are the detailed description of each step in the proposed encryption algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

Example1:

Step 1:CountNo.of characters(N) in the message without space.

Plaintext-frank.

N=5(No.of characters in the message)

Step 2: Convert the plain text into equivalent ASCII code.

102 114 97 110 107

Step 3: Find out the difference between the ASCII code

L1: -2 17 -13 3

Step 4:Take modulus for L1 elements & store it in L2

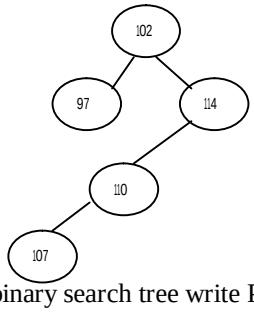
|-2| |17| |-13| |3|

L2: 2 17 13 3

Step 5:From L2 find out the greatest no and store it in G.

G=17

Step 6:From ASCII code value form a binary search tree.



Step 7:From binary search tree write Pre-order & In-order.

Pre-order: 102 97 114 110 107

In-order : 97 102 107 110 114

Step 8:To encrypt the text different keys are used in different levels They are

L1→k1=33

Pre-Order →k2=3

In-Order →k3=2

N , G → k4=32

Each element of L1 subtract form G & Add key k1 with each element of L1

G=17

L1: 17-(-2) 17-17 17-(-13) 17-3

↓

L1: 19 0 30 14

L1: 19+k1 0+k1 30+k1 14+k1

↓

L1: 52 33 63 47

With Pre-order use key k2

102+k2 97+k2 114+k2 110+k2 107+k2

Pre-order: 105 100 117 113 110

With In-order use key k3

97+k3 102+k3 107+k3 110+k3 114+k3

In-order: 99 104 109 112 116

With N& G use key k4

N:N+32=37

G:G+32=49

Step 9:Encryption format- use key k5

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

K5=NGInorderPreorderL1

Encrypted text is

37 49 99 104 109 112 116 105 100 117 113 110 52 33 63 47

Step 10:Convert the ASCII code into character value.

%1chmptiduqn4!?/

The following are the detailed description of each step in the decryption algorithm.

Step 1: Each character in the encrypted text is converted into equivalent ASCII code values.

Encrypted text is : %1chmptiduqn4!?/

37 49 99 104 109 112 116 105 100 117 113 110 52 33 63 47

Step 2: Extract 1st&2nd ASCII code and apply reverse encryption using k4 & store in N, G respectively .k4=32

N=37-k4 So N=5

G=49-k4 So G=17

Step 3: From the ASCII code message extract the ASCII code from 3rd positionupto N elements. Then apply reverse encryption using key k3 and store it in I.

99 104 109 112 116

K3=2

99-k3 104-k3 109-k3 112-k3 116-k3

I: 97 102 107 110 114

Step 4: From the ASCII code message extract the ASCII code from N+3rd position up to N elements. Then apply reverse encryption using key k2 and store it in P.

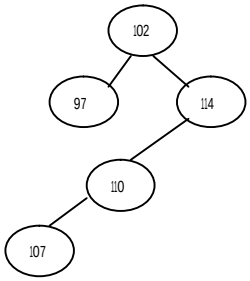
105 100 117 113 110

K2=3

105-k2 100-k2 117-k2 113-k2 110-k2

P: 102 97 114 110 107

Step 5: Construct a binary search tree using I & P.



Step 6:Write pre-order & store it an array A.

Pre-order: 102 97 114 110 107

A:

102
97
114
110
107

Step 7: With the remaining code message apply reverse encryption using the key k1. Then apply the following formula with each ASCII code find out X value.

G-ASCII code=X

Find out X value for all ASCII Code & store it an array B.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

52 33 63 47
K1=33
G=17
52-k1 33-k1 63-k1 47-k1
↓
L2: 19 0 30 14
17-19 17-0 17-30 17-14
↓
-2 17 -13 3

B:

-2
17
-13
3

Step 8: Using the prescribed algorithm rearrange array A elements such a way the difference of
A[0], A[1] should be B[0] &
A[1], A[2] should be B[1] &
A[2], A[3] should be B[2] such as .
A:

102
114
97
110
107

Now can identify the difference of the element is -2 17 -13 3
Step 9: Write the array elements A(ASCII Code).
Now the message is,
102 114 97 110 107

Step 10: Convert the ASCII code into equivalent character value.
Then,
Decrypted result is,
frank
By completion of all these steps in the decryption algorithm the original text is retrieved by the user. In both encryption and decryption, key is more important. Algorithm could be known to everyone but key should be known only to authorize user.

Example2:

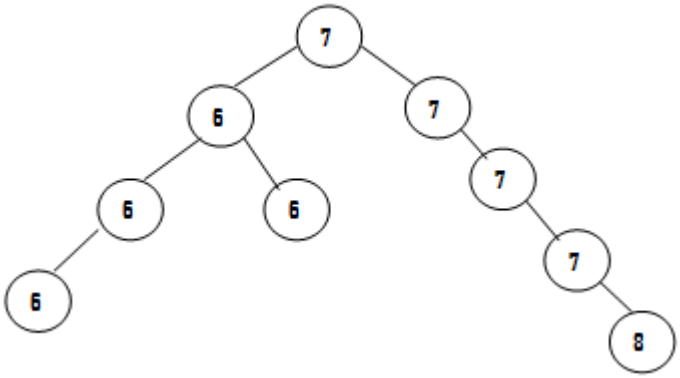
Step 1:CountNo.of characters(N) in the message without space.
Plaintext-hellodear N=9(No.of characters in the message)
Step 2: Convert the plain text into equivalent ASCII code.
72 69 76 76 79 68 69 65 82
Step 3: Find out the difference between the ASCII code
L1: 3 -7 0 -3 11 -1 4 -17
Step 4:Take modulus for L1 elements & store it in L2
|3| |-7| |0| |-3| |11| |-1| |4| |-17|
L2: 3 7 0 3 11 1 4 17
Step 5:From L2 find out the greatest no and store it in G. G=17
Step 6:From ASCII code value form a binary search tree.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014



Step 7:From binary search tree write Pre-order & In-order.

Pre-order: 72 69 68 65 69 76 76 79 82

In-order : 65 68 69 69 72 76 76 79 82

Step 8:To encrypt the text different keys are used in different levels They are

L1→k1=33

Pre-Order →k2=3

In-Order →k3=2

N , G → k4=32

Each element of L1 subtract form G & Add key k1 with each element of L1

G=17

L1: 17-(3) 17-(-7) 17-0 17-(-3)……

↓

L1: 14 24 17 20 6 18 13 34

L1: 14+k1 24+k1 17+k1 20+k1……

↓

L1: 47 57 50 53 39 51 46 67

With Pre-order use key k2

72+k2 69+k2 68+k2 65+k2…….

Pre-order: 75 72 71 68 72 79 79 82 85

With In-order use key k3

65+k3 68+k3 69+k3 69+k3……

In-order: 67 70 71 71 74 78 78 81 84

With N& G use key k4

N:N+32=41

G:G+32=49

Step 9:Encryption format- use key k5

K5=NGInorderPreorderL1

Encrypted text is

41 49 67 70 71 71 74 78 78 81 84 75 72 71 68 72 79 79 82 85 47 57 50 53 39 51 46 67

Step 10:Convert the ASCII code into character value.

)CFGGJNNQTKHGDHOORU/925’3.C

The following are the detailed description of each step in the decryption algorithm.

Step 1: Each character in the encrypted text is converted into equivalent ASCII code values.

Encrypted text is :)CFGGJNNQTKHGDHOORU/925’3.C

41 49 67 70 71 71 74 78 78 81 84 75 72 71 68 72 79 79 82 85 47 57 50 53 39 51 46 67

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

Step 2: Extract 1st&2nd ASCII code and apply reverse encryption using k4 & store in N, G respectively .k4=32

N=41-k4 So N=9

G=49-k4 So G=17

Step 3: From the ASCII code message extract the ASCII code from 3rd positionupto N elements. Then apply reverse encryption using key k3 and store it in I.

67 70 71 71 74 78 78 81 84

K3=2

67-k3 70-k3 71-k3 ……

I: 65 68 69 69 72 76 76 79 82

Step 4: From the ASCII code message extract the ASCII code from N+3rd position up to N elements. Then apply reverse encryption using key k2 and store it in P.

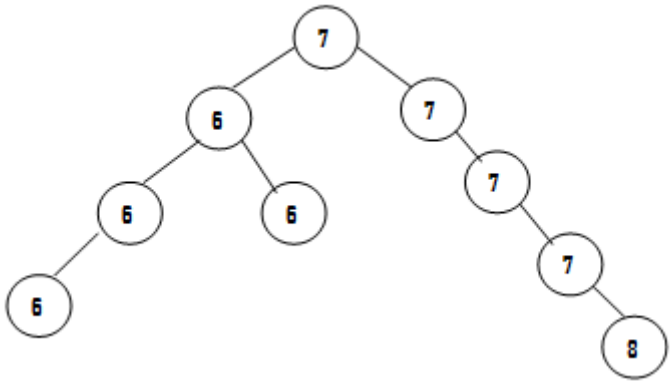
75 72 71 68 72 79 79 82 85

K2=3

75-k2 72-k2 71-k2 ……

P: 72 69 68 65 69 76 76 79 82

Step 5: Construct a binary search tree using I & P.



Step 6:Write pre-order & store it an array A.

Pre-order: 72 69 68 65 69 76 76 79 82

Step 7: With the remaining code message apply reverse encryption using the key k1. Then apply the following formula with each ASCII code find out X value.

G-ASCII code=X

Find out X value for all ASCII Code & store it an array B.

47 57 50 53 39 51 46 67

K1=33

G=17

47-k1 57-k1 50-k1 53-k1……

↓

L2: 14 24 17 20 6 18 13 34

17-14 17-24 17-17 17-20…….

↓

3 -7 0 -3 11 -1 4 -17

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

Step 8: Using the prescribed algorithm rearrange array A elements such a way the difference of
A[0], A[1] should be B[0] &
A[1], A[2] should be B[1] &
A[2], A[3] should be B[2] such as .

72 69 76 76 79 68 69 65 82

Now can identify the difference of the element is 3 -7 0 -3 11 -1 4 -17

Step 9: Write the array elements A(ASCII Code).

Now the message is,

72 69 76 76 79 68 69 65 82

Step 10: Convert the ASCII code into equivalent character value.

Then, Decrypted result is, hellodear

VI CONCLUSION AND FUTURE WORK

Cloud computing is vast warehouse of easily accessible remote resources. It's an emerging trend in this era and developing area also because the people want different access on data depends on the requirement. The emerging trend of the cloud computing also has the security issues. So we need to protect the data from the various particles like Unauthorized access, Data issues, Privacy issues, Trust issues etc[4]. This paper proposed a encryption algorithm for the secure data storage in the cloud. The proposed encryption algorithm is described in detail and the decryption process is reverse of encryption. Here key plays a major role and it acts as primary authentication. By using this encryption algorithm, user ensure that data is stored in the cloud in the secured manner. In future work I believe that data size will be reduced so that can reduce the time complexity.

ACKNOWLEDGMENT

The author would like to thank the dedicated research group in the area of Cloud & Grid Computing , wireless networks at the Dept of MCA,AIMIT, Mangalore, India, for many stimulating discussions for further improvement and future aspects of the Paper. Lastly but not least the author would like to thank everyone, including the anonymous reviewers.

REFERENCES

1. P. Subhasri and Dr. A. Padmapriya"Multilevel Encryption for Ensuring Public Cloud",IJARCSSE,vol 3, Issue 7, July 2013
2. Dr. L. Arockiam, S. Monikandan "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm" International Journal of Advanced Research in Computer and Communication Engineering, vol 2,Issue 8,August 2013.
3. "Data Security in cloud" PROTECTING BUSINESS-CRITICAL INFORMATION IN PUBLIC, PRIVATE, AND HYBRID CLOUD ENVIRONMENTS.
4. Dr A. Padmapriya,"Cloud Computing:Reverse Caesar Cipher Algorithm to Increase Data Security"IJETT,vol 4,
5. issue 4,April2013.
6. John Harauz,LoriM.Kaufman, Bruce potter "Data security in world of cloud computing" buy IEEE computer and reliability societies,jul/aug 2009 pp61-64.