IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-17, May 2019 E-ISSN: 2347-2693

Authentication and Encryption in Cloud using Linear Algebra

T. Aruna

Dept. of Computer Applications, Islamiah Women's Arts and Science College

Corresponding Author: arunavelu6l@gmaill.com

Available online at: www.ijcseonline.org

Abstract— Cloud computing a new concept of Modern World and it combines all the service models and technologies together to deliver IT enterprise**.** The objective of this algorithm is to provide the security to end user to protect files or data from the unauthorized user. Privacy is an important issue for any technology through which unauthorized user can access your file or data in a cloud. I have presenting an encryption algorithm to deal with the privacy problems in cloud computing and protect the data stored in the cloud.

Keywords—Computing, Encryption, Decryption

I. INTRODUCTION

The Cloud Computing means provides computing over the internet and this world is basically inspired by the cloud. The word cloud is a metaphor for internet. In this data is stored at remote location and available on demand. It allows clients to use applications without installation the file at any computer with internet facility. By data out sourcing user can get the information from anywhere more efficiently and has no burden on data storage and avoid the extra expenses on software hardware and information resources and data maintenances and used more efficiently.

II. LINEAR ALGEBRA

The linear algebra uses basic matrix multiplication. So the alphabets are converted into numbers. Each letter from a to z is assigned a digit from 0 to 25 such as a=0, b=1 and z=25. As there are 26 letters the base is used as 26.

The total encryption process is divided into three parts:
i. Preparing the plain text
ii. Preparing the key
iii. Encryption.

i. Preparing the plain text
First each letter in the message is converted into numbers such as a=0, b=1 and so on. Then the number should be written in columnar form. The number of letters in each column depends on the key matrix size. Suppose the key matrix is 2*2, Then each column of plain text having two elements only. For 3*3 the total number of elements in the plain text should be multiple of 3 Otherwise append necessary elements to make it multiple of 3. Suppose there are 19 elements in the plain text then in each column there are 3 elements but in the last column there is only one element. So append 2 more elements in the last column.

ii. Preparing the key
Every letter in the key is also assigning the number like message. Then the number should be written in row wise. The number of letters in each row depends on the matrix size. Suppose the key matrix is 2*2, then each row having two elements only. The key matrix is always square matrix.

The key either it may be a character or numeric if it is numeric it can be taken has as it is otherwise the alphabet key will be converted into number based the alphabet table value. Then write these numbers in matrix form.

iii. Encryption
The encryption is the multiplication of the key matrix and plaintext matrix. The number used for the letters are base 26. So mod 26 is used to generate the cipher text.
Cipher text=key*plain text mod 26
C= kp mod 26

Once the matrix multiplication operation computed then we will get numbers here the numbers are converted into letters.

III. LINEAR ALGEBRA ENCRYPTION

The encrypted information can be stored in a tree based on their values.

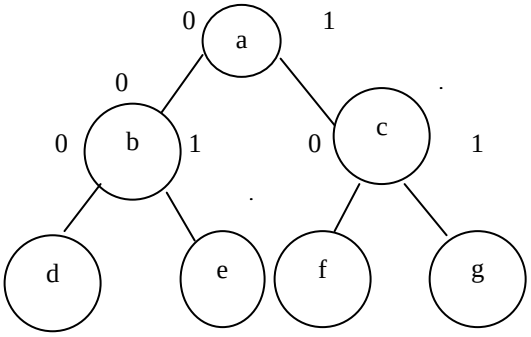

Figure 1 Diagram for Alphabets along with their Positions

i. Steps for Encryption

1. Enter Encrypted user Details in a tree
2. Arranging the odd and even position separately
3. Insert redundancy bit 111111(6 times 1 for security)
4. This makes the user name and password as unreadable.

ii. Steps for Decryption

1. Receive data along with redundancy bits.
2. Start from a, assign left sub trees as 0 and right sub trees as 1.
3. In this redundancy bit given are '111111' (6 times 1) which is used to represent the redundancy bit from the received data.
4. Take the actual data after detecting the redundancy bit from the received data.
5. Assign the alphabet to a numeric values in the received data
6. Rearranging according to odd and even position in alphabetic order.

IV. LINEAR ALGEBRA DECRYPTION

To convert the cipher text into plain text again we have to perform matrix multiplication.

The inverse of key matrix is multiplied by the cipher text matrix to generate the plain text matrix to calculate the inverse of the key matrix

$P=k^{-1} * c \bmod 26$

1. Here we first compute $k^{-1}$and mod 26
2. Then find multiplicative inverse of d
3. Cipher text is multiplied by key
4. We will get the plain text

V. PROPOSED METHOD

We have presenting an algorithm using linear algebra and tree table .By using this method the user log in can be encrypted in two different methods .First the user data can be encrypted using linear algebra. For that the user should enter the numeric key Based on the key value the user log in data can be converted into encrypted form. Then we are applying one more encryption method .Which is the Encrypted values can be placed in a binary tree based on the tree table .The alphabets which are even can be placed separately and odd characters can be placed separately and we have to add 6 bit redundancy code for these alphabets.

For decrypting this value first we should remove redundancy bit. Then we have to apply tree traversal .It may produce some character information it can be placed in a matrix form and we have to apply inverse matrix. Then we have to use numeric key for modulus operation and we will get the original information.

VI. ENCRYPTION ALGORITHM USING LINEAR ALGEBRA

Step1. The user log in can be placed as a matrix in columnar form.
Step2. Get the numeric key for encryption.
Step3. Numeric key can be arranged as a row matrix.
Step4. Apply matrix multiplication.
Step5. Convert the result matrix into numbers using alphabets table.
Step6. The number can be arranged in a sequence.

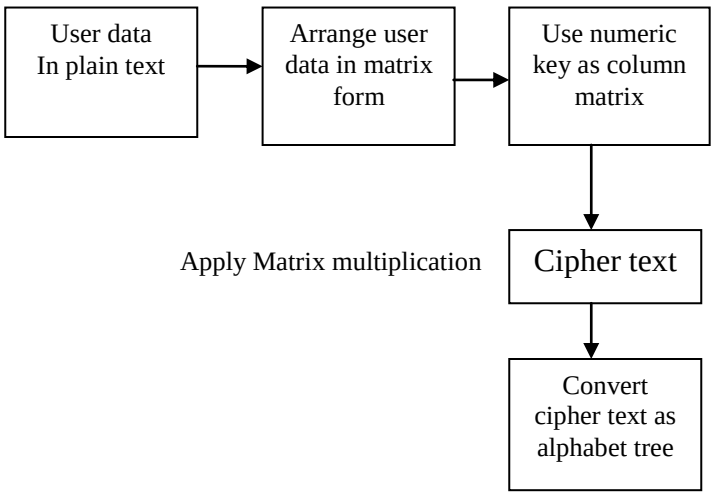

Figure 2.Encryption using Linear Algebra

VII. ENCRYPTION ALGORITHM USING TREE TABLE

Step1: A design tree for alphabets a to n is given in table 1
Step2: Starting from a, assign left sub tree as 0 and right sub tree as 1.
Step3: Repeat the procedure up to n.
Step4: Arrange the alphabets according to even and odd positions as given in above example.
Step5: In that odd position alphabet should be arranged first and even position at last.

Step6: Assign values to the alphabet in the user name as given above a=0, b=00, c=01 etc.
Step7: Insert redundancy bits between the values of the user name.
Step8: Store the data user name with added redundancy bits.

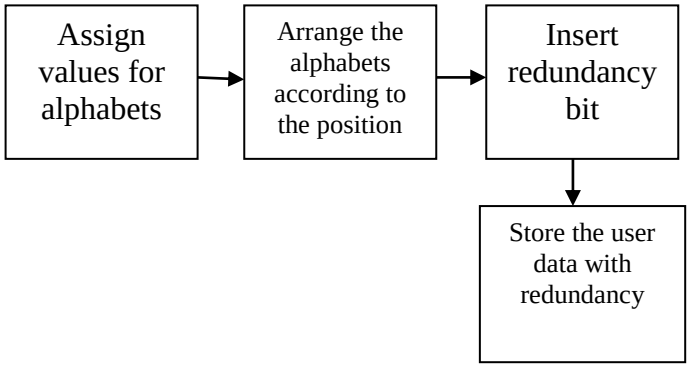

Figure 3. Diagram for Encryption using Tree table

VIII. DECRYPTION ALGORITHM FOR ENCRYPTION USING TREE TABLE

Step1.Retrieve data along with redundancy bit.
Step2. Start from a assign left sub tree as 0 and right sub tree as 1.
Step3.Remove the redundancy bit
Step4.Take out actual data after detecting the redundancy bit.
Step5. Assign the alphabet to a numeric values.
Step6. Rearrange according to odd and even position in alphabetic order.

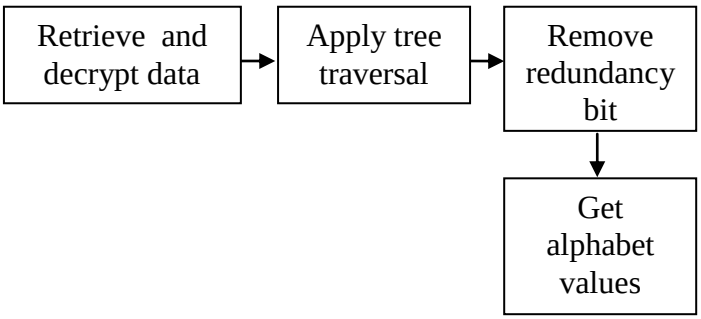

Figure 4. Diagram for Decryption Using Tree table

IX. DECRYPTION ALGORITHM USING LINEAR ALGEBRA

Step1. Apply matrix multiplication
Step2. The inverse of key matrix is multiplied by corresponding values of user data
Step3. Apply modulus operation.
Step4. Receive original data.

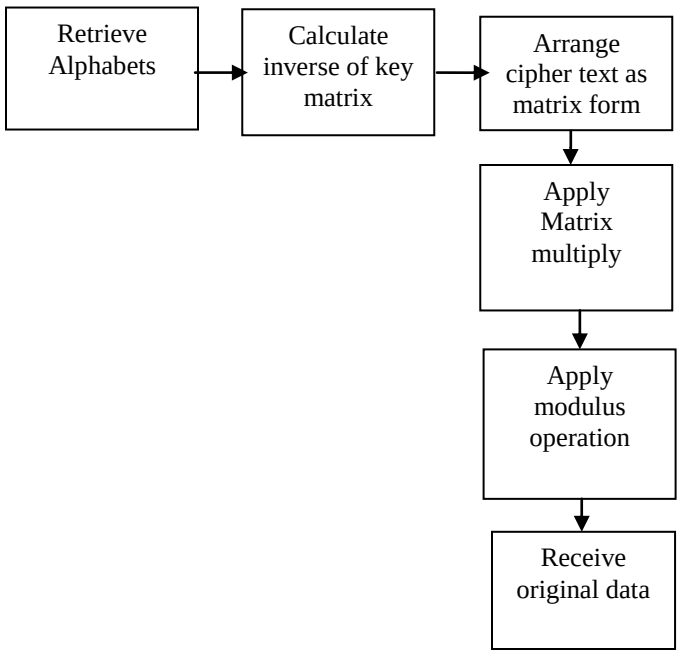

Figure 5: Diagram for decryption using linear algebra

X. CONCLUSION

The most valuable asset in cloud computing is user data. The protection of user data security is extremely vital and considerable because if data security is not protected, the cloud will practically lose its meaning. Therefore security solutions in this system are constantly updated. A very important part of data security in cloud is authentication, so that unauthorized people will be prevented to enter and merely authorized people will be allowed to enter.

This technique of password authentication provides secure authentication which is better than the usual password technique. An attempt has been made to just authenticate and then use cryptography to further secure authentication.

Future Enhancement
In Future the above approach can be enhanced further by including an integrity check mechanism.

REFERENCES

[1]. Arjunkumar ,Byung Gook Lee , AnuKumari "secure storage and access of data in cloud computing" .IEEE on ICTC, 2012.
[2]. M.M .Auxilia and K. Raja, "semantic based access control for ensuring data security in cloud computing", IEEE conference on reader, Communication and computing 2012
[3]. Meer SoheilAbolghasemi , MahadiMokkarmi "using location based encryption to improve the security of data access in Cloud computing", IEEE conference on advances in computing communications and informatics,2013.
[4]. Rao Srinivasa and V .Nageswara Rao , "Cloud computing an overview ", computing,pp71-76,2009
[5]. Kulkarni .G "A security aspects in cloud computing", Computer Engineering, IEEE,PP 547-550,2012.

