Authenticate Communication with Adjacency Matrix using OTP(One Time Transaction) Method

Gurusharan Kaur[1], Dr. Rizwana Jamal[2]

[1] *Department Of Mathematics , Barkatullah University, Bhopal*
[2]*HOD , Department Of Mathematics, Safia Science College, Bhopal*

Abstract

Graph theory has many applications in computer science. But it can also be used to make the data secure. Sometime it is used in networking for many purposes. Cloud computing provide user many services like SAAS, IAAS and PAAS. But with many benefit still cloud providers are not too much confident about the security aspects. As for the data storage, cloud data center depends upon third party involvement. So there is need of an algorithm that can authenticate sender and receiver before any transaction between user and third party. The Proposed algorithm uses the adjacency matrix to make the data secure. OTP is one of the attractions used before any transaction.

Keywords: Cloud computing, SAAS, IAAS and PAAS

I. Introduction

Cloud computing is a new technology that provides user many conveniences using the internet and central remote servers to maintain data and applications. For cloud users data are accessible from anywhere any time. Users have also not to worry about software updating.

User authentication is needed for access of data in the network. At ancient time secret data or code is used for hiding and giving security to information. In user authentication method, user has to proof the authenticity of him for various transactions on cloud computing also.

Authentication process divided into Token based authentication, Biometric based authentication and Knowledge based authentication. Most of the web applications include alphanumeric password as well as graphical password.

In cloud storage system third party are included. When client wants to fetch the information, he or she can access data server through a web based interface. Similarly for uploading also data on cloud also user have to proof the identification. The server then response either by sending the files back to the client or allows the client to access and manipulate the files on the server directly.

II. Literature Survey

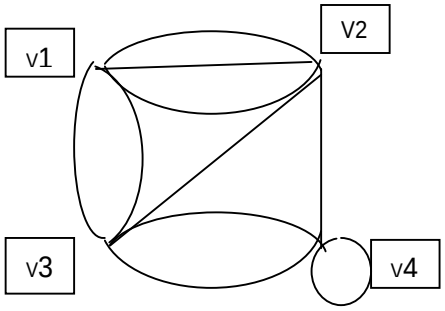
Users of elliptic curve cryptography (ECC) suggest that ECC requires much smaller keys as compared to other conventional public key cryptosystems. Neal Koblitz and Victor Miller recommended the use of elliptic curves in public key cryptography. An elliptic curve utilization is used therefore also supports faster encryption and decryption.

The elliptic curve cryptography Diffie-Hellman Algorithm described with the example of alice and bob. Alice and Bob share the secret key that is confidential between them and impossible for a third party to discover. [6]For making the data secure they proposed cloud with graphical security by means of image password. They proposed

algorithms which are based on selection of username and images as a password. By this paper they are trying to give set of images on the basis of alphabet series position of characters in username. Cloud is provided with graphical password authentication.

III. Proposed Algorithm

A graph and its adjacency matrix



	V1	V2	V3	V4
V1	**0**	**3**	**2**	**0**
V2	**3**	**0**	**1**	**1**
V3	**2**	**1**	**0**	**2**
V4	**0**	**1**	**2**	**1**

Adjacency Matrix

Algorithm to share Security key

1. Find adjacency matrix of the given graph which is shared between sender and receiver.
2. Decide the new value to be used in the matrix for a particular transaction.(Like V3 , V4)
3. Convert the value V3, V4 to its octal representation.
4. Perform AND operation on the received value.
5. Result is again converted into octal representation which is security key to be send by the receiver as OTP (one time password) received in the mobile number of the sender.
6. Receiver and sender both perform same operation with the shared matrix with the new value for a particular operation.
7. Transaction performs if the OTP of sender and receiver match.

Example 1

1. Find adjacency matrix of the given graph which is shared between sender and receiver.
2. Decide the new value to be used in the matrix for a particular transaction.(Like V3 , V4)
   i.e let decide v3 and v4 so data is

0	**2**
2	**1**

3. Convert the value V3, V4 to its octal representation.

000	**010**
010	**001**

4. Perform ADD operation on the received value.

000010

010001

———

010011

5. Result is again converted into octal representation which is security key to be send by the receiver as OTP (one time password) received in the mobile number of the sender.
   i.e 010011 to octal is 23.
6. Receiver and sender both perform same operation with the shared matrix with the new value for a particular operation.
7. Transaction performs if the OTP of sender and receiver match.

Example 2

1. Find adjacency matrix of the given graph which is shared between sender and receiver.
2. Decide the new value to be used in the matrix for a particular transaction.(Like V2 , V3)
   i.e let decide v2 and v3 so data is

0	**1**
1	**0**

3. Convert the value V3, V4 to its octal representation.

000	**001**
001	**000**

4. Perform ADD operation on the received value.

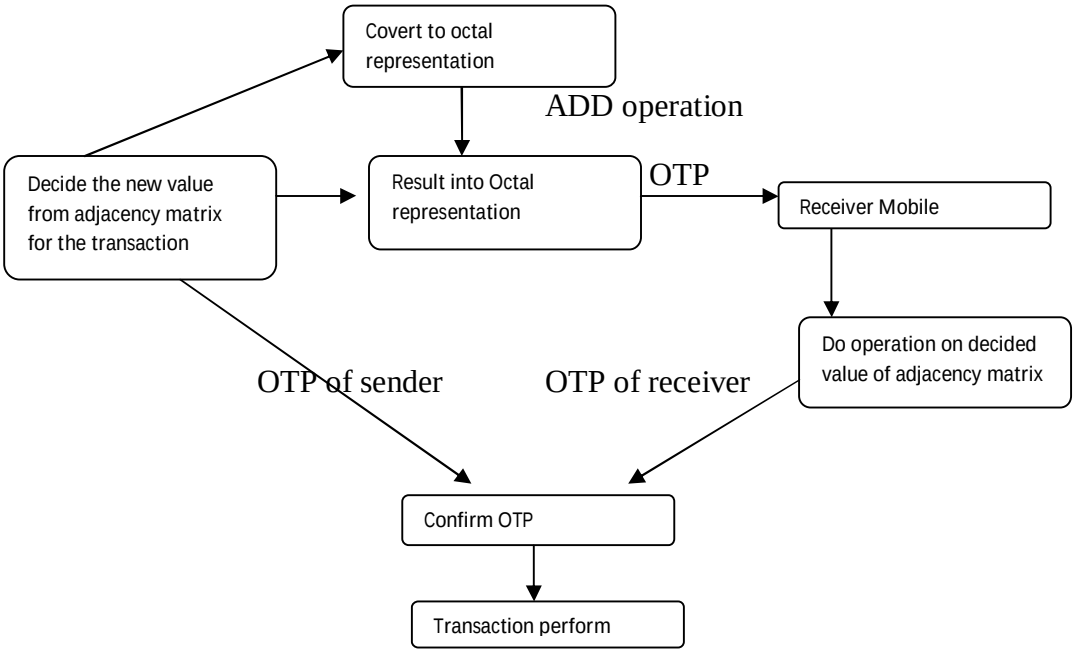
000001

001000

———

001001

5. Result is again converted into octal representation which is security key to be send by the receiver as OTP (one time password) received in the mobile number of the sender.
   i.e 001001 to octal is 11.
6. Receiver and sender both perform same operation with the shared matrix with the new value for a particular operation.
7. Transaction performs if the OTP of sender and receiver match.



State Diagram of Authentication method

IV. Conclusion and Future enhancement

Proposed algorithm can be used in highly sensitive data transaction like Bank transaction for net banking etc. Some time it is beneficial in transaction like data transfer for other beneficiary account within the same bank, data transfer for other beneficiary account outside the bank. Algorithm provides double security system with OTP confirmation which makes the transaction more secure.

V. REFERENCES

[1] A Survey on Recognition-Based Graphical User Authentication Algorithms
[2] Authentication Using Graphical Passwords: Basic Results Susan Wiedenbeck Jim Waters ,College of IST Drexel University Philadelphia, PA, 19104 USA
[3] Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice Susan Wiedenbeck Jim Waters College of IST Drexel University Philadelphia
[4] Graphical Passwords, FABIAN MONROSE AND MICHAEL K. REITER, August 5, 2005
[5] N. Koblitz, " Elliptic Curve Cryptosystems ", Mathematics of Computation, vol. 48, pp. 203- 209, January 1987.
[6] Secure Storage and Access of Data in Cloud Computing Arjun Kumar , Byung Gook Lee, HoonJae Lee, Anu Kumari, ©2012 IEEE
[7] Security Analysis of Graphical Passwords over the Alphanumeric Passwords by G. Agarwal ,1Deptt.of Computer Science, IIET, Bareilly, India 2,3 Deptt. of Information Technology, IIET, Bareilly, India 27-11-2010
[8] V. Miller. "Uses of Elliptic Curves in cryptography". RYPT'85, LNCS 218, pp 417-426, 1986.
[9] W. Stallings. Cryptography and Network Security: Principles and Practice. (3rd ed.). Prentice Hall, Upper Saddle River, New Jersey, 2003,
[10] Wassim Itani Ayman Kayssi Ali Chehab, "Privacy as a Service:Privacy-Aware Data Storage and Processing in Cloud Computing Architectures", Eighth IEEE International Conference on Dependable, 2009.