Privacy Protection Through One Time Password And Transaction Authentication Number In Transcation Processing System

Lakshmi Priya. P[1], Mythili. S[2], Nivetha. M[3]
Department of CSA
[1,2,3] Bharathiar University/Sri Krishna Arts And Science College/Coimbatore, Tamil Nadu, India

Abstract- *Although huge methodologies are in market to generate One Time Password (OTP), day to day hackers are creating techniques to smash the code and track the OTP. In this paper, a consistent method of generating One Time Password is proposed. Based on the credentials from the source and the length of the message, id of the client, two 8 bit binary code are created and converted into decimal through CB2D Procedure, to create two 3 digit decimal values. The decimal values are then multiplied by the 3X3 Vedic multiplier. The outcome of the Vedic multiplier is the One Time Password. Also here, since the destination plays the role of showing the interest either to accept or deny the message from the source, the percentage of false authentication is reduced than the traditional techniques.*

Keywords- One Time Password, Vedic Multiplier.

I. INTRODUCTION

As OTP’s are valid for only one session, it is less vulnerable to the attacks. But today’s incomparable steadfast technology growth has even made the OTP’s less secure. The OTP’s are generated based on the previous generated One Time Password, synchronization time between the server and the client. SMS OTP is secured only if the cellular network is highly secured.

Mobile based Trojans are created for breaking the code in Smartphone to track the confidential information. So, a strong multifactor authentication which works eventually during the attempts of unguarded trials is necessary. Also, an efficient methodology that works fast even during clumsy mathematical operations is required to generate the One Time Password.

From the ancient mathematical sutras, Vedic multiplier is opted for generating the One Time Password in rapid manner. In olden days, when there is no calculators to compute complex values, this Vedic multipliers are used to compute the same. This Vedic multiplier is especially from Urdhva tiryakbhyam that reduces the time of multiplication and even deletes the duplication and unwanted multiplication steps. Nowadays Vedic multipliers are used in the area of image processing, signal processing, wireless communication, audio and video processing etc. Vedic multiplier is also used for encryption in the RSA, DES algorithms.

II. RELATED WORK

Hussain (2016) turned up with the concept of graphical One Time Password by combining recognition and draw based graphical passwords. He used key-board entry. He reviewed the common user- authentication mechanisms and conducted a review of graphical password schemes. They assessed mechanisms offered by banking’s system and user’s perception. Then he developed GOT Pass and evaluated its security and usability.

Swapna et al.(2016) developed a two level password authentication system. They combined the features of existing authentication schemes. User credentials are stored in database by speech to text mechanism. Two OTP’s are generated in web part and application side. Both the generated OTP’s are checked and if a match is found, then the generated OTP is sent to smart phone of user. Their results are so user friendly, easy to understood and more secure.

They used Vedic multiplier to implement the mathematical part in the RSA algorithm and experimented that the efficiency of the RSA algorithm is increased in terms of Speed when compared to the traditional techniques.

Himika et al (2012) integrated image based authentication and Message authentication code based one time password is used for high level of security. Initially the messages are authenticated using image passwords and then the Hash Message authentication code.

Neha et al. (2013) developed synchronous stream cipher. They used images instead of passwords as secret keys. The image is connected to random text field and the image is vector is built. Taking the image vector as input, the keystream is generated using hash function. They performed XOR operation of keystream bytes and text bytes. Then the bytes are connected to its equivalent hexadecimal. From the hexadecimal, eight characters were selected and stored with session, then the characters are encrypted using ECC which gives the One Time Password.

III. PROPOSED METHODOLOGY

When a source wants to initiate a communication to the destination, the source or the client can login the details in the database and make the request for the certificate authority. The Certificate authority checks the database for the credentials and it is converted to the 8 bit binary value. The length of the message and the id are then converted to the 8 bit binary value. The 8 bit binary values are converted to decimal through CB2D procedure. This two 3 digit numbers are multiplied using the Vedic multiplier to generate the OTP and it is send to the source. If the destination is interested for communication, it sends signal otherwise the port for the communication will be closed.

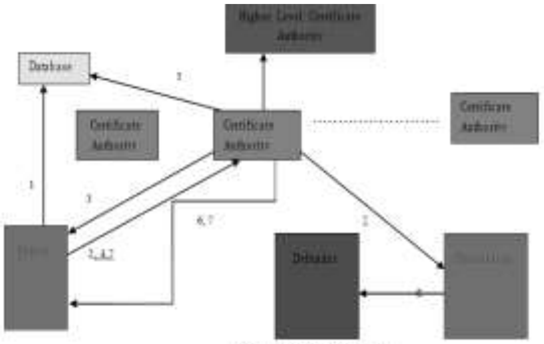


Figure1: Block Diagram

1. Source files the credentials in the database.
2. Source request the certificate to the certificate authority.
3. CA request the ID from the source.
4. Source grants the ID.
5. CA validates the credentials.
6. Generated OTP is given to the source (if match found).
7. If the same OTP is received back, certificate is issued to source and a photocopy is sent to the destination.
8. Destination accepts if interested else close the port and report to the defender.

3.1 Algorithm for certificate issue

1. Client login the credentials in the database to enter the network.
2. Source needs to communicate with destination D.
3. Source request for a certificate to Certificate Authority (CA).
4. Certificate authority asks for the credentials from the source.
5. Source enters the credentials.
6. Certificate authority checks with the database.
7. If match found, OTP is generated and send to source.
8. If the same OTP is received from the source, the certificate authority issues the certificate to the source and a copy of the same will be given to the destination claimed by the source.
9. If the destination is interested, it sends a signal to the source and the Source initiates the communication.
10. If D is not fascinated, it will close the serial port and inform to its guard.
11. The defender report it to the higher level Certificate authority.

3.2 Algorithm for OTP generation

Input:

1. Source enters the credentials and it is converted to 8-bit binary value.
2. From the source, CA extracts the length of the message and the id of the client
3. Both inputs are converted to 16 bit binary value, which is then converted to a denary.
4. Both the denary's are then converted to 8- bit binary value.
5. The 8-bit binary value is a input to the conversion of binary to decimal CB2D.
procedure to get a 3 digit decimal value.
6. This 3 digit decimal value and the 3 digit value got from the source as credentials are multiplied using a 3x3 Vedic multiplier.

Output:

The output of the 3x3 Vedic multiplication generates a 6 digit OTP which is send to the source.

3.3 Vedic Multiplication

For example, Suppose if the 3 digits are 132 and 214

Step a) Right Side Vertical

1 3 2
2*4=8
2 1 4

Step b)Right and Middle Criss Cross

1 3 2
3*4+2*1=14
2 1 4

Step c) Middle Vertical and Side Criss Cross

1 3 2
1*4+2*2+3*1=11

2 1 4

Step d) Left and Middle Criss Cross

1 3 2
⋈ 1*1 + 3*2=7
2 1 4

Step e) Left Side Vertical

1 3 2
↓ 1*2=2
2 1 4

Now from the up write all the values, (from the right fill the value) 8, then 14 so put 4 and add 1 to 11, there it becomes 12 so take 2 and add 1 to 7, there it becomes 8 and the last value 2. So the OTP generated is 28248.

3.4 Working of Mapping box

Consider the input to Mapping box is 10011101 and split into four two bits say 10,01,11 and 01. Take two bits and map with the mapping` box taking 1 as row and 0 as column. Likewise rest of the bits are mapped with the mapping box respectively to get a total of our bits and then this four bits are expanded to get 8 bit binary value which is then converted to 3 digit decimal number.

IV. EXPERIMENTAL RESULTS

A mesh topology is created with 100 nodes and the Ns2 parameters are shown in Table 1. In this paper, experimental evaluation is presented for the packet transmission, Vedic multiplication for generation of OTP and Certificate. NS2 is used for the simulation of network and it is the Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries.

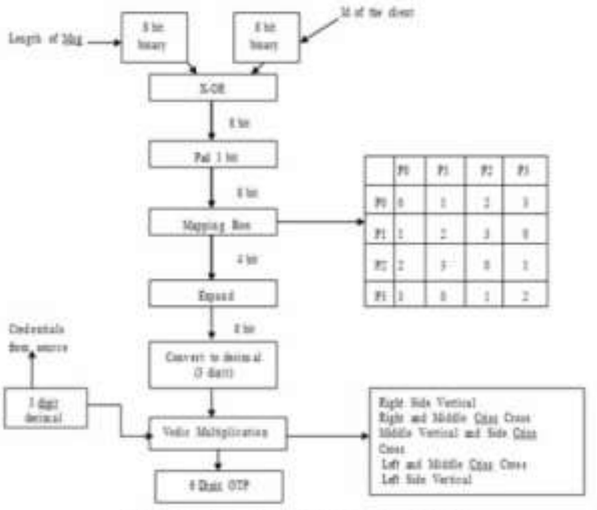
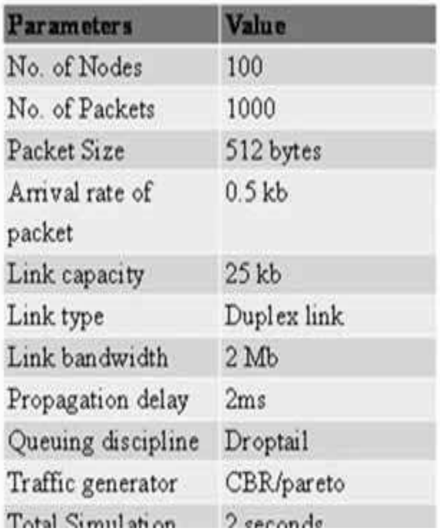


Figure 2: Architecture of OTP generation using Vedic Multiplier

Quite a good number of experiments pursued are experimented with a purpose of quantifying the impact of proposed system on the performance of the OTP generation.

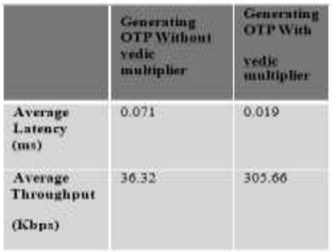
Precisely, these experiments have demonstrated the efficiency of the proposed techniques in the performance of Packet transmission. It is also noteworthy that the performance of the proposed approach is compared with the table it is clear that average latency is decreased when OTP is generated with vedic multiplier than the traditional technique. Also an intense increase is achieved in generating OTP with vedic multiplier than the conventional techniques.

Table 1: NS2 Parameters



Parameters	Value
No. of Nodes	100
No. of Packets	1000
Packet Size	512 bytes
Arrival rate of packet	0.5 kb
Link capacity	25 kb
Link type	Duplex link
Link bandwidth	2 Mb
Propagation delay	2ms
Queuing discipline	Droptail
Traffic generator	CBR/pareto
Total Simulation	2 seconds

Table 2:Average Latency, Throughput Vs Vedic Multiplier



	Generating OTP Without vedic multiplier	Generating OTP With vedic multiplier
Average Latency (ms)	0.071	0.019
Average Throughput (Kbps)	36.32	305.66

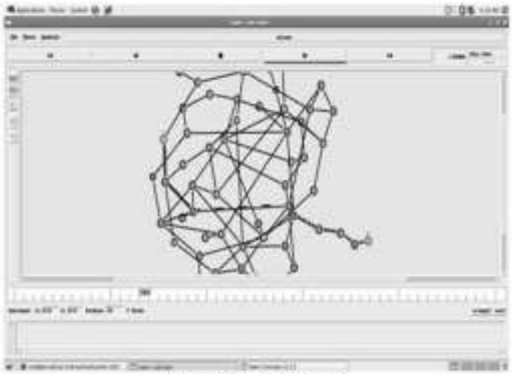


Figure 2:Simulation Graph

From figure 2, it is clear that there is free Flow of packets with less delay and high throughput.

V. CONCLUSION

Even though OTP is measured as the most secured authentication methodology, still its getting hacked by the unauthorized persons. So for every minute, different methods are evolved to make the OTP more secure. In this paper, a new method is developed in such a way that only after proper certification from Certificate Authority, OTP is generated and send to the required source. This gives double the times authentication. Also, for generating OTP, ancient method of vedic multiplier is used for manipulation. Also, the delay is highly decreased and throughput of the network is improved by implementing vedic multiplier in generating OTP.

REFERENCES

[1] Dhanashri R. Kadu , Dr.G.P.Dhok,” A novel effiecient technique for data security using vedic mathematics”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 4, Issue 5, May 2015,pp 87-93.

[2] Swapna Borde, Gauri Satish Tambe, Suchita Ramdas Tambade,” Two Level Password Authentication System”, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 5, Issue 2, March 2016,pp:95- 101.

[3] Hussain s. Alsaiari,” Graphical one-time password authentication”, school of computing, electronics and mathematics faculty of science and engineering(ph.d thesis)

[4] Himika Parmar1 , Nancy Nainan2 and Sumaiya Thaseen,” Generation of secure one-time password based on image authentication”, itcse, cs & it 07, pp. 195–206, 2012.

[5] Neha Vishwakarma, Kopal Gangrade,” Secure Image Based One Time Password”, International Journal of New Innovations in Engineering and Technology”, Volume 6Issue 1– October 2016,pp:6-11

[6] Cryptography and Network Security by William Stallings, Third Edition, Pearson Education

[7] Cryptography and Network Security by Atul Kahate, Tata McGraw Hill,2003.