Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

One Time Password System for Security over Clouds

Neha Sharma* Gurukul Engineering College, Kota Aff. Rajasthan Technical University Kota, Rajasthan, India

Kiran Gautam Gurukul Engineering College, Kota Aff. Rajasthan Technical University Kota, Rajasthan, India

Praveen Nagar SEC, Jhunjunu, Rajasthan Aff.Rajasthan Technical University Kota, Rajasthan, India

Abstract*— In this article the implementation and analysis of one time password process is carried out to secure the data on cloud. To download the file which was uploaded by client to his account from cloud, client has to log in again to his account and the window and the files which were uploaded earlier are shown in the window. In the download window the client has to click on the file icons to be downloaded by client. Once client clicks on any of the icon a onetime password (OTP) is generated and mailed to the client, which has to be entered by the client on desired place. This OTP is valid for the time period of the current session, once session expires the OPT will not be accepted by the system, a separated OTP will generated for every file to be downloaded by the client. If OTP entered by client is correct, file is available for download.

Keywords*— OTP-one time password, Ant Colony Algorithm, Genetic Algorithm, Elliptic Curve, Blowfish Algorithm and EABC

I. INTRODUCTION

Cloud computing is a growing technology example that shifts the technological and computing concepts into utility-like solutions. This technology provides a large pool of services without any initial investment on set up. The cloud computing concept eliminates the need for hiring and training the IT professionals but at the same time Cloud computing comes with the threat of theft, misuse or discloser of data of the costumer organization accidentally or deliberately because the data of the costumers of a cloud service providers is available at remote server, which may be shared between a number of clients. Such type of technology also increases the client's flexibility by immediately taking over the services and basic resources when needed. The major aspects to think about are security and privacy concerns which are considered the primary threats to a wide utilization of clouds. The new concepts that are included in clouds are multi-occupancy, resource sharing and outsourcing; demand a very high security level.

In recent times, the significance of ensuring the remote data integrity has been highlighted by the following research works [1–5]. These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols [6–8] for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited. Researchers proposed several methods of security of data over cloud.

OTP-onetime password is the method to avoid data unauthorised access to our account. It gives an additional security to uploaded data. Network security deals with large number of devices to provide them secure access. User has to use its valid identification scheme to access the services provided by network. Unauthorized or unwanted user has no right to access the secure services provided on network. It provides security for both public which can be access by all users and private networks which can only be access by legitimate users. Network security performs authentication procedure by username and passwords. Network security is wide area of research today. Number of areas comes under their research is Mobile networks , Wireless Networks, Sensors Networks, Wireless sensors networks, Mobile Ad hoc networking, cryptography , Information security , Mobile security , wireless communication etc. Lot of research can be done on these areas, many algorithms are developed or modify , many security techniques are developed for providing the security in these areas. Cryptography is main tool in network security. It works on three attributes are Confidentiality, integrity and availability. Confidentiality means the authorized person is same as it claims to be , Integrity deals with the concept that data is received same as it is send by the sender and Availability deals with that the devices should available for providing network security. Cryptography use many Encryption and Decryption algorithm for dealing with confidentiality and Hash algorithms , MAC algorithms and Digital signature algorithms to deal with data integrity.

A. ONE TIME PASSWORD

One time password generator is an algorithm that generate new random password every time. It works as a machine or algorithm that takes input from users and produce new password that is different from previously generated password. Network security deals with authenticate the user with id and password but this method is vulnerable to many attacks so

for secure authentication every time new password is used whether the previous password is stolen or misplace. One time password generator is main element of One Time Password system used for generating the generating random passwords other elements of this system is client authentication and Server authentication. Popular OTP used are HOTP based on SHA-1.Hash algorithms used are MD4, MD5 but these are vulnerable to attacks. Another OTP is based on Ping Pong-128 stream cipher in which Ping Pong-128 algorithm is used to generate the random numbers.

One time password is secured because:
1. It can't used twice or
2. It is not reversible to reach at source back.

It mainly deals with the two elements
1. Key
2. Counter

OTP system generates one password at a time and provides it to client for authentication.OTP send password to client by SMS service, by phone or by written. Password is secure by the application on client mobile.
In our work we purpose a One Time Password generator using Ant Colony Algorithm, Genetic algorithm with Elliptic Curve. Section 3 problem formulation. Chapter 4 explain about our work plan along with its timelines

II. LITERATURE REVIEW

A. ANT COLONY ALGORITHM

It is the research field of Marco Dorigo et al. during its master thesis in 1991.Afrter their research many version of ant colony algorithm are developed. It is the algorithm largely applied to many combinatorial optimization problems. After the ant colony developed as metahueristic many variant of algorithm are developed.ACO depends upon the foraging behavior of ants of finding the food source. Ant finds the food source by traversing the shortest path and deposits the chemical substance pheromone on it. Second time when another ant wants the food then it chooses that path having high pheromone value. Ants communicate with each other through chemical substance called pheromone [4].

1) Build the Solution: In this every ant builds their solution by traversing the graph. Ant on one node selects the node according to the probability:

$$p_{xy}^{k} = \frac{(\tau_{xy}^{\alpha})(\eta_{xy}^{\beta})}{\sum_{y \in \text{allowed}_y}(\tau_{xy}^{\alpha})(\eta_{xy}^{\beta})}$$

Where Ʈxy is the amount of pheromone on edge x, y. ηxy is the heuristic value which is describe as 1/dxy (dxy is the distance between edge x and y). α and β are the relative influence on parameters Ʈ and η. An ant repeat the previous step to find the valid tour of its each iteration and find the solution which is iteration best tour. All ant find their best tour after their each iteration, solution of each ant is compared and uses the best so far solution.

2) Update the Pheromone: After ant finds their tour they deposit pheromone substance on that path which is the process of updating the pheromone value. The pheromone values are more on paths which are traverse by more number of ants. For more effectiveness of more pheromone on good paths some amount of pheromone is removed from the path to avoid the bad quality solution. So pheromone updating consists of pheromone evaporation as negative feedback and pheromone updating as positive feedback. The rule is:

$$\tau_{xy} \leftarrow (1-\rho)\tau_{xy} + \sum_{k} \Delta\tau_{xy}^{k}$$

Where $(x,y) \in L$,L is set of all edges , ρ is the evaporation rate , k is number of ants. Pheromone update by ant k is $\Delta\tau_{xy}^{k}$. This is defined as:

$$\Delta\tau_{xy}^{k} = \begin{cases} Q/L_k & \text{if ant } k \text{ uses curve } xy \text{ in its tour} \\ 0 & \text{otherwise} \end{cases}$$

Where Lk is the tour length constructed by ant k and Q is a constant.

B. GENETIC ALGORITHM

Genetic Algorithm is the research field of John Holland based on the principle of natural genetics. It maintains some initial population and generate a solution from that population by applying their operators of selection, crossover and mutation to find a optimize solution GA use the variables in the form of binary string {0, 1} because it is optimal solution. In GA the population is choose called as chromosomes and from that population offspring is produced by applying the crossover and mutation operator. Parents choose from the population for producing offspring are according to their fitness value and fitness value of offspring is also calculated so that less fit offspring should be deleted *[9][10]*.

Stages in Genetic Algorithm
The different stages of GA *[9]* are:

1) *Initial Population of GA:* First step in GA is to select the population of chromosomes. The fitness function of all these chromosomes is calculated. According to the different research the initial population size should be random. Other possible solution is the „seeding" of initial population i.e. according to some research initial population of GA should be the output of some other heuristic technique produces good results.

2) *Selection of Chromosomes:* The parents or chromosomes that are to be select for reproduction is choose according to their fitness value. Most common method is choosing according to the fitness so that more fit parent has more chance for reproduction.

3) *Crossover:* After selecting the parents of high fitness value next step is to perform the crossover operation. In this few chromosomes of one parent is replace with other parent so that new offspring should be generated having some characteristics similar to that of their parents.

Example we have two parents P1 and P2 as:
P1 = 1 0 0 1 0 0 0 1
P2 = 1 1 0 1 1 0 0 0

And after crossover the offspring"s are as: X3 = 1 0 0 1 1 0 0 0 and X4 = 1 1 0 1 0 0 0 1.

4) *Mutation:* The next step after crossover is mutation. In some cases there is no need for crossover directly mutation is performed. In case after crossover two same offspring"s are produced then random bits from one offspring is mutated to produce different offspring. Suppose we have offspring X3 = 1 0 1 1 0 0 0 and we want to mutate its 4 and 8 bit then after mutation new offspring is X5 = 1 0 0 0 1 0 0 1.

C. *ELLIPTIC CURVE ALGORITHM*

An elliptic curve E takes the general form as:

$$E: y2 = (x2+ax+b) \bmod P$$

Where a, b are in the appropriate set (rational numbers, real numbers, integers mod p, etc.) and x, y are elements of the finite field GF (p), satisfying 4a3 + 27b2 != 0 (mod p)….(5) and p is known as modular prime integer making the elliptic curve finite field*[15]*.
There are two basic group operations on elliptic curve which are point addition and point doubling.

1) *Point Addition*: Addition means that given two points E and their coordinates, P = (x1, y1) and Q = (x2, y2) belongs to E (GF (p)), we have to compute the coordinates of a third point R such that:
P + Q = R
(x1, y1) + (x2, y2) = (x3, y3)
This is the case where we compute R = P+Q and P≠Q.Point R"s coordinates (x3 ,y3) also belongs to E (GF(p)).
$\lambda = (yp - yq) / (xp - xq)$
$xr = [\lambda 2 – xp – xq] \bmod p$
$yr = [-yp + \lambda (xp-xr)] \bmod p$

2) *Point Doubling*: Point doubling is the addition of a point P on E to itself to obtain another point R. This is the case where we compute P + Q but P = Q. Hence we can write R = P + P = 2P.
$\lambda = (3x2p + \alpha) / 2yp$
$xr = [\lambda 2 – 2xp] \bmod p$
$yr = [-yp + \lambda(xp – xr)] \bmod p$

D. *BLOWFISH*

Bruce Schneider designed blowfish in 1993 as a fast, free alternative to existing encryption algorithm. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. The Blowfish algorithm has many advantages. It is suitable and efficient for hardware implementation and no license is required [*16]*. The elementary operators of blowfish algorithm include table lookup, addition and XOR. The table includes four S-boxes and a P-array. Blowfish is a cipher based on feistel rounds, and the design of the F-function used amounts to a simplification of the principle used in DES to provide the same security with greater speed and efficiency in software. Blowfish is a 64 bit block cipher and is suggested as a replacement for DES. Some specifications of Blowfish algorithm are as follows-

1. A 64 bit blocks cipher with a variable key length.
2. There is a P-array and four 32-bit S-boxes. The P-array contains 18 of 32-bit sub keys, while each S-box contains 256 entries.

3. The algorithm consists of two parts: a key-expansion part and a data-encryption part.
4. Key expansion part converts a key of at most 448 bits into several sub keys array totaling 4168 bytes.
5.The data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation and a key and a data dependent substitution.
6. All operators are XORs and additions on 32-bit words.
7. The input is 64 bit data element.

The process of Sub key generation is illustrated as follows-
1. Initialize P array and S boxes with Hexadecimal digits of Pi.
2. XOR P-array with the key bits (i.e., P1 XOR (first 32 bits of key), P2 XOR (second 32 bits of key).
3. Use the above method to encrypt the all-zero string.
4. This new output is P1 and P2.
5. Encrypt the new P1 and P2 with the modified sub keys.
6. This new output is now P3 and P4.
7. Repeat the above steps until we get all the elements of P array i.e. P1, P2.

The encryption algorithm for Blowfish is illustrated as follows: 1

Table I: Blowfish Encryption algorithm

1.Divide X into two 32-bit Halves: XL, XR
2.For I = 1 to 16
XL = XL ⊕ Pi
XL = F(XL) ⊕ XR
Swap XL AND XR
3.Swap XL AND XR (undo the last step)
4. XR = XR ⊕ P17
5.XL = XL ⊕ P18
6. Concatenate XL and XR

III. PROBLEM FORMULATION

After studying the papers and how the OTP works, we formulate our problem as One Time Password can be used to provide security over cloud to avoid unauthorised login. One time password process is carried out to secure the data on cloud. To download the file which was uploaded by client to his account from cloud, client has to log in again to his account and the window and the files which were uploaded earlier are shown in the window. In the download window the client has to click on the file icons to be downloaded by client. Once client clicks on any of the icon a onetime password (OTP) is generated and mailed to the client, which has to be entered by the client on desired place. This OTP is valid for the time period of the current session, once session expires the OPT will not be accepted by the system, a separated OTP will generated for every file to be downloaded by the client. If OTP entered by client is correct, file is available for download.

IV. RESULTS AND DISCUSSION

To download a file, client has to log in again and the window and the files which were uploaded earlier are shown in the window. In the download window the client has to click on the file icons of the file to be downloaded as shown on the screen (Fig. 1).

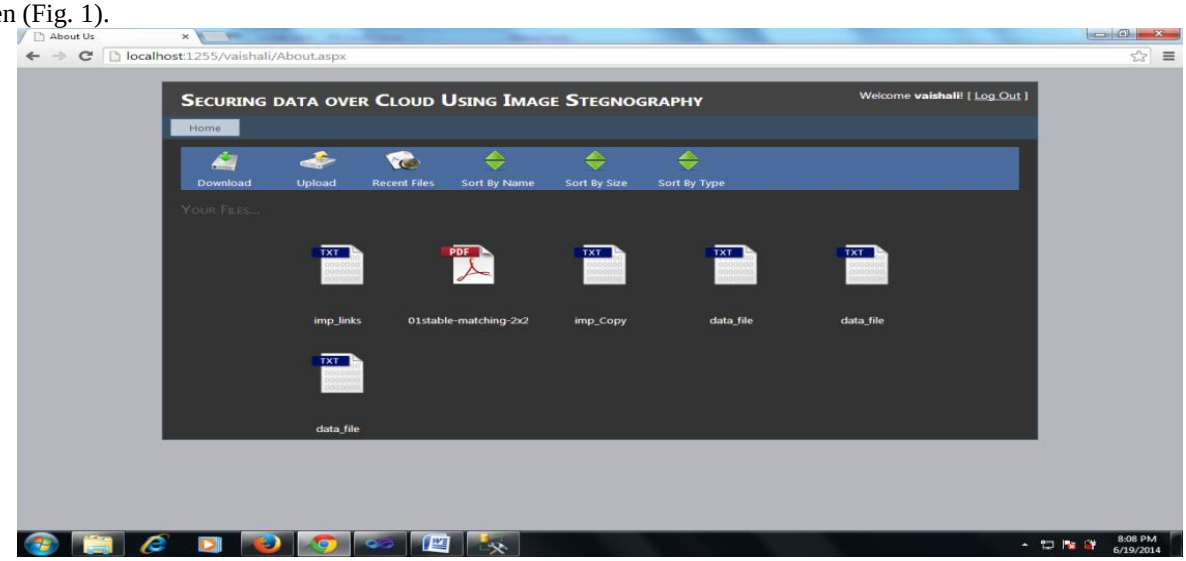

Fig. 1 The download window

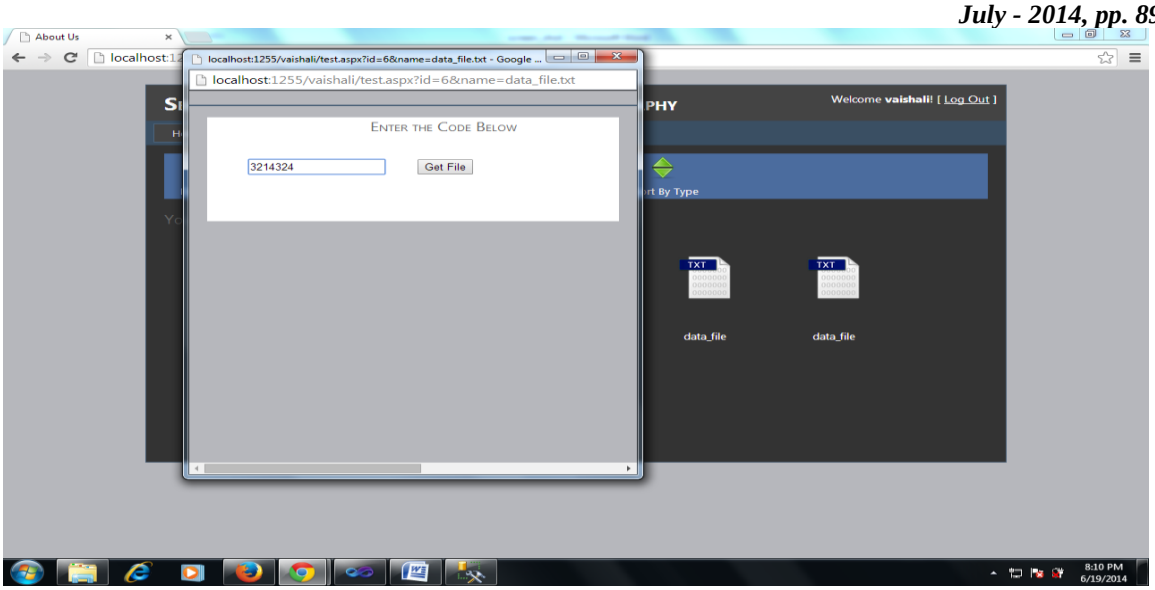

Fig. 2 The verification procedure using onetime pass word

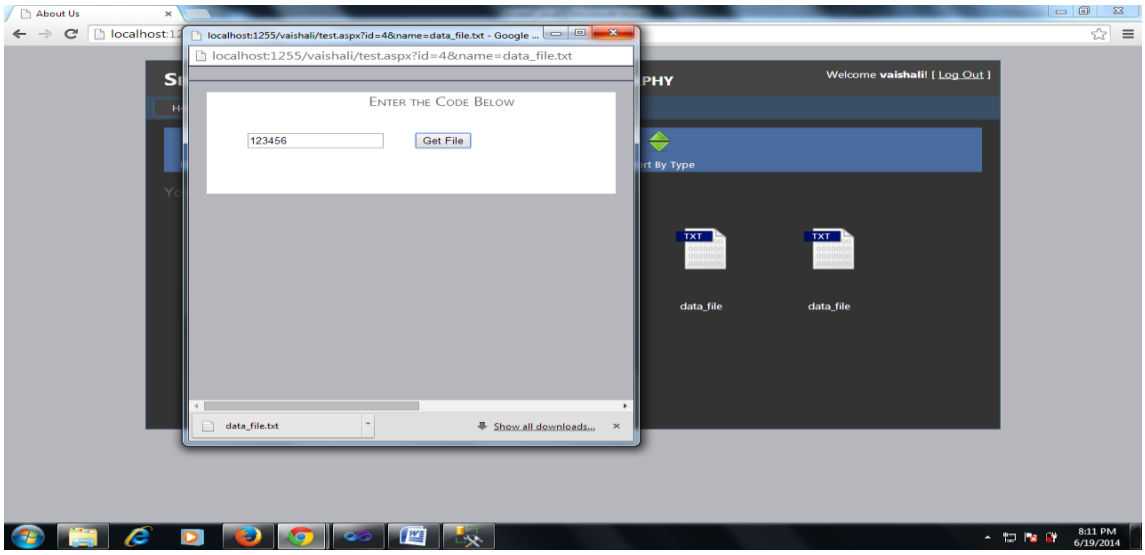

Fig. 3 Download options after verification

Once client clicks on any of the icon a onetime password (OTP) is generated and mailed to the client, which has to be enter by the client on this screen (Fig.3). This OTP is valid for the time period of the current session, once session expires the OPT will not be accepted by the system, a separated OTP will generated for every file to be downloaded by the client. If OTP entered by client is correct, file is available for download (Fig 4).

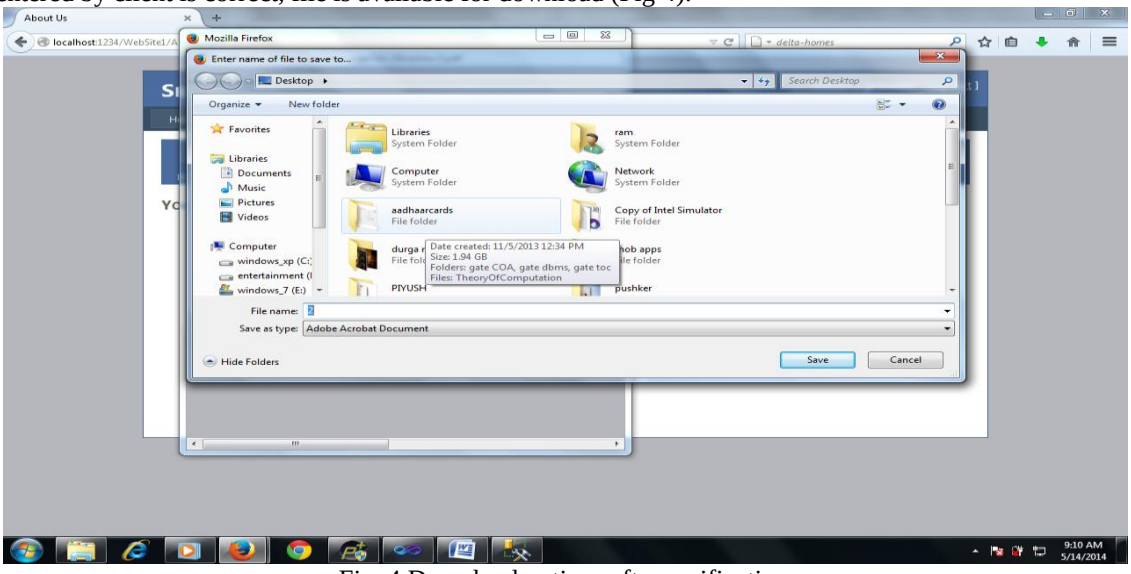

Fig. 4 Download options after verification

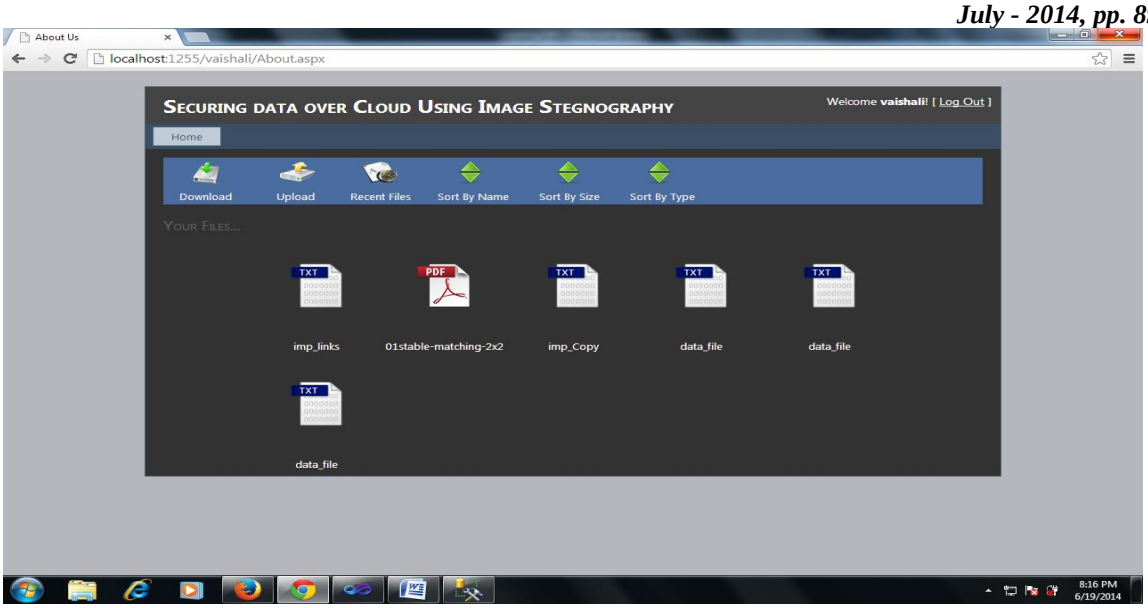

Fig. 5 File options in the window

Client may download the file to the desired location of his/her system (Fig 5).

V. CONCLUSIONS

One time password is an efficient technique that generate random password each time for users. If user lost their pervious password then there is no need of worry for them because OTP give them new password for each session.OTP prevent user id from replay or eavesdropping attack. Earlier OTP is generated using HMAC , One way hash function and Ping Pong stream cipher , in which input is given to OTP generator as challenge and it generate random password. In our work we propose a method of generating OTP generator using Genetic algorithm with elliptic curve algorithm. In future more how to provide more security in this approach and on secure authentication between client and server.

ACKNOWLEDGMENT

The author is thankful to Mr. Navdeep Kumar, M.Tech. Scholar at University College of Engineering, Kota, Rajasthan, India for giving good suggestions during my work.

REFERENCES

[1] Horowitz, Sahni, Rajasekaran, "Fundamentals of Computer Algorithms".
[2] Young Sil Lee, HyoTaek Lirn, HoonJae Lee ,"A Study on Efficient OTP Generation using Stream Cipher with Random Digit".
[3] Bayalagmaa Davaanaym, Young Sil Lee, HoonJaeLee, SangGon Lee and HyoTeak Lim," A Ping Pong One-Time-Password system in Java application".
[4] Sjoerd van Egmond , "Dynamic Ant Colony Optimization for the Traveling Salesman Problem"
[5] Neha Jain Jasvinder Pal Singh," Modification of Ant Algorithm for Feature Selection".
[6] KUANG Xiangling, HUANG Guangqiu2, "An optimization algorithm based on ant colony algorithm".
[7] Dewen Zeng, Qing He, Bin Leng, Weimin zheng, Hongwei Xu, Yiyu Wang, Guan," An Improved Ant Colony Optimization Algorithm Based on Dynamically Adjusting Ant Number".
[8] Zhiguo Liu , Tao Liu, Xiue Gao," An Improved Ant Colony Optimization Algorithm Based on Pheromone Backtracking".
[9] Colin Reeves, School of Mathematical and Information Sciences," GENETIC ALGORITHMS".
[10] Melanie Mitchell, Santa Fe Institute, "Genetic Algorithms: An Overview".
[11] L. Fua, D. Sunb, L.R. Rilettc," Heuristic shortest path algorithms for transportation Applications: State of the art".
[12] Andrew V. Goldberg, Chris Harrelson," Computing the Shortest Path: A Search Meets Graph Theory". [13] Nadira Jasika, Naida Alispahic, Arslanagic Elma, Kurtovic Ilvana, Lagumdzija Elma, Novica Nosovic," Dijkstra's shortest path algorithm serial and parallel executionPerformance analysis".
[14] Pengfei Guo , Xuezhi Wang , Yingshi Han," The Enhanced Genetic Algorithms for the Optimization Design".
[15] MeltemKURT , Tank YERLiKA Y A," A New Modified Cryptosystem Based on Menezes Vanstone Elliptic Curve Cryptography Algorithm thatUses Characters' Hexadecimal Values"
[16] Monika Agrawal, Pradeep Mishra , "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm".
[17] Hamid Mehdi, "EABC: Data Encryption Method Based on Circle".
[18] http://i1-win.softpedia static.com/screenshots/One-Time-Password-Generator_1.png
[19] http://www.networkworld.com/subnets/cisco/chapters/1587052466/graphics/01fig02.jpg

[20] http://srvloc.org/wp-content/uploads/2012/01/computernetworksecurity.jpg
[21] http://www.yorku.ca/mack/IWC99-f2.jpg
[22] http://www.hextoascii.info/img/ascii_chart-ascii_to_hex_binary_decimal-table.png
[23] http://en.wikipedia.org/wiki/One-time_password
[24] http://en.wikipedia.org/wiki/Ant_colony_optimization_algorithm
[22] D. M‟Raihi, M. Bellare UCSD, F. Hoornaert VascoD. Naccache Gemplus O.Ranen Aladdin December 2005 Network Working Group, Request for Comments: 4226,Category: Informational," HOTP: An HMAC-Based One-Time Password Algorithm".
[23] D. M‟Raihi Verisign, Inc.,S. Machani Diversinet Corp.,M. Pei SymantecJ.,Rydell Port wise, Inc. May 2011, Internet Engineering Task Force (IETF), Request for Comments: 6238 Verisign, Inc. Category: Informational ISSN: 2070-1721 Diversinet Corp." TOTP: Time-Based One-Time Password Algorithm".
[24] N. Haller , Bellcore , C. Metz Kaman Sciences Corporation , P. Nesser Nesser & Nesser Consulting, M. Straw Bellcore February 1998,"Request for comments : 2289 A One-Time Password System".

