Journal of Computer Science and Cybernetics, V.32, N.4 (2016), 303–318
DOI 10.15625/1813-9663/32/4/8744

PASSWORD ENCRYPTION BASED ON DYNAMIC GRAPH LABELING PRIORITY GENERATION (D.G.L.P.G.) TECHNIQUE

[1]SANJAY KUMAR PAL, [2]NUPUR CHAKRABORTY

[1]*Dept. of Computer Sc. and Applications, NSHM College of Management and Technology, Kolkata – 700053; sarbojay@gmail.com*
[2]*Dept. of Computer Sc. and Applications, NSHM College of Management and Technology, Kolkata – 700053; nupurc1995@gmail.com*

Abstract. The formalization of speedy technical environment due to the progression in hardware technologies is consistently stimulating the terror of brute force attacks and challenging even the strongest encryption algorithms. Current security requisition can never be truly fulfilled if security system of any real world system is dependent upon only static protection mechanism. A dynamic approach must have to be adopted to integrate dynamic protection mechanism along with static protection mechanism. Within in this scope both static and dynamic password encryption mechanisms face the danger of being attacked. Here we have expressed our concern for dynamic password security system which acts as shield against Man in the Middle attacks. In this paper we propose a password encryption technique based on the "Dynamic Graph Labeling Priority Generation (D.G.L.P.G.) Technique" and "Dynamic False Node Insertion (D.F.N.I) Technique" for dynamic password. The algorithm has achieved very low space complexity and time complexity which is $O(\log n)$. The emerged technique fits itself in the boundary of the present requisition and is flexible enough to expand its magnitude with the amplifying needs up to the boundary mark of the presented algorithm.

Keywords. Encryption, graph labeling, false node, dynamic insertion, priority generation technique, actual node, dynamic password.

1. INTRODUCTION

Graph labeling is the process of assignation of labels to vertices, edges or both of a graph "G", where labels are conventionally symbolized as integers. A graph $G = (V, E)$ with a function of V to a set of labels is called as "Vertex labeled graph". Only information security at the system level at the sender or receiver site can never ensure the preservation of information. There is always a threat of Man in the Middle (MiM) attacks that can severely harm the effective communication between two parties. As in the active eavesdropping the attacker makes false connection between the actual communicating parties, controls the communication and extracts the necessary information from them. If this necessary information is user's password whether static or dynamic which is encrypted using weak encryption mechanism then the alarming situation of being attacked by hackers can be felt very easily. The main causal agent of MiM attacks are:

ARP Cache Poisoning;

DNS Spoofing;

Session Hijacking;
SSL Hijacking.

1.1. Address resolution protocol cache poisoning (ARP)/ARP spoofing/ARP poison routing

In this attack methodology the intruder transmits (spoofed) Address Resolution Protocol (ARP) message onto a local area network with the objective to connect their MAC address with the IP address of the another victim. So any packet intended to the victim's IP address will be sent to the intruder.

1.2. DNS spoofing/DNS cache poisoning

In this attack methodology the intruder inserts data in the Domain Name System (DNS) resolver's cache. As an outcome a false IP address is returned by the name server that causes distraction in the network traffic to the intruder's computer.

1.3. Session hijacking/cookie hijacking

In this attack methodology the intruder utilizes the cookies used for a valid computer session establishment and gets an illegal access to the information or services in the computer system and controls the session.

1.4. SSL hijacking

Secure Socket Layer (SSL) are the cryptographic protocols responsible for facilitating communication security over a computer network. But now days they are also facing the security challenges. One of the recent evidence is that Comodo Registration Authorities, InstantSSL.it and GlobalTrust.it were hacked. And false certificates were generated for the likes of Google, Hotmail, Yahoo!, Skype, and Mozilla [22]. According to the recent security centered happenings in the technical world, Lenovo has launched computers with preloaded software Superfish Visual Discovery that is specifically responsible for installing self generated root certificate into the windows certificate store. In the next step the SSL certificates proposed by HTTPS sites are replaced with its original certificate [14].

1.5. Brute force attack/exhaustive key search

It is a kind of a cryptanalytic attack that takes advantage of flaws of encryption system and starts guessing all possible keys/passwords until the actual one are discovered. With the advancement in the hardware technologies the brute force attack is becoming more powerful [7].

1.6. Dictionary attack

It is a type of attack that works on the principle of guessing the decryption key or passphrase by continuously trying all possible alternatives in order to crack the end user password.

The changing needs of this changeable world becomes quiet unmanageable if stringent approach is taken towards designing security system. Hence imposing the whole burden on only static passwords is a kind of invitation to the malicious activities of adversaries that are performed with the support of immensely powerful hardware devices to resolve the puzzle of generation of ciphers. Moreover phishing attacks are also there. The sensitivity of the situation looks for a dynamic password technique or One Time Password technique (OTP). These OTPs have the capability to combat with phishing attacks [9]. OTPs are valid for a small duration of time gives a very small chance to the intruders to perform their unlawful tasks but even a single point of vulnerability can cause a major harm. So it is essential to adopt a strong encryption mechanism, even for this dynamic password or OTP as the increasing speed of processors is enhancing the disruptive power of attackers. This essentiality is also expressed by Fred Cheng in one of his workings which employs Rubbing Encryption Algorithm (REAL) to implement a Mobile-based and a Cloud-based OTP Token design which is resistible to Man-in-the-Middle seed tracing attacks [4]. The thrust of dynamic password demand generated with time has resulted in evolution of several kinds of OTP or dynamic password techniques each of which focuses on several critical issues. One-Time Password authentication scheme using a smart card is focused on lowering the Client side computational costs and communicational costs and to increase the limit of login times [12]. With the target of building more strong security shield time and location based One Time Password authentication scheme is proposed [8]. OTP is applied in diverged ways in several application fields. Two-factor authentication in cloud computing can be accomplished with aid of OTP [23]. End-to-End authentication between IoT devices/ applications can be achieved using two-factor authentication mechanism which exploits One Time Password authentication scheme based on elliptic curves [19]. For securing confidential information as personal health records in cloud One Time Passwords can be used [16]. Hence demand of dynamic passwords is increasing day by day in various arenas. And moreover it is needed to strengthen the static password based security mechanism. But only its dynamic nature cannot ensure its robustness even it is dynamic in nature, it must be encrypted using a strong encryption algorithm. In this paper we are proposing a dynamic password encryption technique based on the Dynamic Graph Labeling Priority Generation (D.G.L.P.G) technique and Dynamic False Node Insertion (D.F.N.I.) technique with the objective to preserve the actual significance of the dynamic password where password can contain number, lower case or upper case character, and symbol. That is even if the intruder comprises the network security and gets access to the confidential information like dynamic password he/she will fail to make use of it because of the strong dynamic encryption mechanism that works as a protective shield and preserves the privacy of the dynamic password. This paper is concentrated mainly to deal with Man in the Middle attacks where attacker could imitate himself/herself as any one of the legal communicating parties. The seventh section of the presented paper has explained the usability of the proposed technique to generate a secure session that is completely resistible to Man-in-the-Middle attacks. The actual implementation could take bit more time in session generation, due to the 3-way Client initiated authentication principle. But it is necessary for both legal communicating parties to ensure the legitimate presence of each other.

2. COMPARATIVE STUDIES OF THE EARLIER PIECES OF WORKS

Analyzing encryption techniques is an intense evaluation which needs a 360^o evaluation. Our study over password Encryption techniques does not only limit its scope to dynamic passwords but also extends itself to static kind of passwords. As in today's trend security can never be guaranteed by only one means, flexibility is essential, to open up the door of possibilities oriented to build up a more secure system. Sometimes static password encryption techniques used to get choked with the complexities associate with the high security urges. But if as a support the system contains dynamic password generation mechanism also embedded into it then the burden which is only imposed on static password generation mechanism can be reduced. As a sample the most recent static kind of 3D password encryption technique can be considered which yet ensures very high level of protection but at the cost of slight inconvenience to user in the situation when user need to remember all 3D action sequences which becomes an excruciating job when numbers of objects or events are more in number and activities are performed in a haphazard manner [10, 17, 15, 1, 6, 3]. Its space complexity as well as time complexity is quite high which is $Am+Bn$ where m represents the time needed to communicate with the system and n represents the time needed to process each algorithm in 3D environment [17]. From the implementation point of view the current 3D password technique demands the application of 3D modeling techniques. 3D designs are one of the parameter that decides the mystification of the password. So the concreteness of the technology expects a good design at the cost of complexity in implementation. The above facts initiates us to think in a diverge way in terms of distributing the load of ensuring a top level security to both kinds of password security mechanisms static as well as dynamic, however filtering is always preferred, therefore selection process is followed even for dynamic password encryption technique. A technique can never be called as robust if it excels only in one dimension. Presence of correct proportion of all factors that are necessary for existence of a technique in its actual implementation in real world is required. These factors are dependency of the parameters of the technique on other external factor and which type of changes they exhibit with the changing external factors in terms of security level, associated complications in implementation, time and space complexity, user friendliness. Thus the basis taken here for doing comparison considers all previously mentioned factors so that an economic dynamic password generation technique can be developed. Comparison between the proposed technique and recent available techniques begins with the One Time Password generation technique that depends upon the four digits Personal Index Number (PIN) provided by the bank to the customers at the time of registration for internet banking or mobile banking. Whenever a specific user initiates a transaction it is used for producing sub- keys for the different rounds of feistal network. Each time using the same Personal Index Number for a particular user for generating the core factor of the encryption technique that is sub-keys makes the algorithm, exceedingly dependent on it [20]. The Graphical One Time Password (GOTPass) based authentication relies on a sequence of secret images and a pre chosen input format. Dependency of OTP upon pre chosen input format is a point of vulnerability as well as storage and maintenance of secret images is also a cumbersome task [2]. OTP based two factor authentication using mobile phones in which multiple OTPs are generated from an initial seed where the initial seed is generated on the basis of communications partners' unique parameters, yet eliminates the requirement of sending SMS-based OTPs to users and diminishes the constraints caused by the SMS system but whether it includes secure initial

authentication setup during the transfer of initial secret seed must be checked out [5]. In the other category of One Time Password generation techniques which are based on the image based authentication, the first sample illustrates a technique in which key of the algorithm is username and Image Based Password. Here instead of images the categories of the images are stored in Image Identification Set. If same key is used each time, then if an intensive analysis will be done over cipher texts produced by a particular user then in this case the logic behind algorithm can be detected. To overcome this situation if regularly Image Based Passwords will be updated then the other interrelated factors of the algorithm will also need to be modified [13]. The second sample illustrates a technique in which one time password is generated using image selected at the time of registration with SHA 512 encryption with the arbitrarily selected text fields provided at the time of registration. Storing images for each user increases huge load if number of users are really large [21]. Usage of biometric feature such as "Score Level Fusion" makes One Time Password more secure. In this methodology the weights of multiple Biometric properties are compared against the images in the database and a weight used to be found. Based on the weight found user's legitimacy is checked if the weight is above threshold then the user is legitimate else not. Next to this an another level of verification is done on the basis of one time password which is produced using a cryptographic technique in which final fused weight value is exploited as a private key. Yet a high security level is achieved but the cost of complexity in implementation, in verification process, in storing and maintaining huge database can never be ignored [18]. The proffered technique attempts its best to develop an economic dynamic password generation technique which will be also encrypted to 256 nodes long cipher before transmission in communication network. Supreme ease in terms of choosing password is given to the user. It makes this technique quite user friendly. It means that password can be even single character long but will still possess high brute force resistance capability which is independent of the length of the password, however in general password length should be at least four characters long. Everything is dynamic so there is no storage and maintenance burden. Additionally the delineated technique bears low space complexity as well as time complexity which is $O(\log n)$, where n is the length of the password. The actual implementation could take bit more time in session generation, due to the 3-way Client initiated authentication principle. But it is necessary for both legal communicating parties to ensure the legitimate presence of each other for strong network security. Therefore on the basis of overall evaluation done it can be concluded that presented algorithm is the right balance of all necessary factors that a current dynamic password encryption algorithm requires.

3. BASIC TERMINOLOGIES

3.1. Actual node

Actual Node signifies those vertices that are able to generate the Euler graph depicting the actual dynamic password.

3.2. False node

False Node signifies those vertices of a graph that are not responsible for generating the Euler graph representing the actual dynamic password given by the user but are intended

to make alterations in the graph formed by Actual Nodes to misguide the intruder.

3.3. D.G.L.P.G technique

The soul of the proposed dynamic password encryption technique is based on the above mentioned technique and degree of randomization provided by this technique in each turn of its application. This technique assigns priorities to the Actual Nodes as per the formula:

$$\log e_{10}^{ki} \,. \tag{1}$$

Here i can vary from 1 to 5 signifying the variations in the selected attribute as per the requisition of the algorithm. The value obtained from the formula is refined in various ways to generate the actual priority value for the nodes.

3.4. Randomization

It is the degree with which the unique priority assigned to each actual node by D.G.L.P.G. technique vary within each iteration as per the given dynamic password and in the next iteration with an another dynamic password.

3.5. D.F.N.I. technique

This is the mechanism which involves the alteration of configurations of Actual Nodes in the original Euler graph (made up of only Actual Nodes) by inserting False Nodes in between them at the positions specified by the sorted sequence of priorities generated by the D.G.L.P.G technique generating modified Euler graph (made up of Actual and False Nodes).

3.6. Shifting

As per D.F.N.I. technique insertion of False Nodes always causes shift in the Actual Node positions as well as shift in the False Node insertion position with the exception of the first False Node insertion position. This phenomenon is termed here as "Shifting".

3.7. Mixed array

It is the array representing the modified Euler graph generated after D.F.N.I. technique is applied on the original Euler graph.

3.8. Finalpwd array

It is the array which will be containing total 256 nodes consisting Actual and False Nodes with the majority of False Nodes that represents the extended modified Euler graph working as a shield to brute force attacks.

3.9. Priority array

It is the array which will be containing the priority values assigned to each Actual Node.

3.10. Prioritypositionarray

It is the array which will be containing the priority positions with respect to each Actual Node.

3.11. False array

It is the array which will be containing the False Node insertion positions but these positions can change accordingly with the Shifting property of the algorithm.

3.12. Actual array

It is the array which will be containing the Actual Node insertion positions but these positions can change accordingly with the Shifting property of the algorithm.

3.13. Actual array

It is the array which is exploited while decryption to retrieve the actual user given dynamic password.

4. TECHNIQUE OF THE PROPOSED ALGORITHM

Technique of the presented algorithm is illustrated in three subsections. In which first subsection deals with Mixed array insertion position. Second subsection deals with fundamental steps associated with the DGLPG technique. Third subsection deals with key insertion position foundation.

4.1. Fundamental steps involved in finding mixed array insertion position

Store all values of the attributes current day, current month, current minute, current second, current hundredth of seconds in the respective variables $k1, k2, k3, k4$ and $k5$ from the current date and time system.

Generate unique values by inserting $i = 1, 2, 3, 4$ in the equation (1).

For each generated unique value extract the value after decimal up to first three. Addition of all these extracted values is stored as sum.

Generate dynamic value which is the additional result of value 60 and value of the attribute $k5$.

From the sum dynamic value is subtracted.

After subtraction the modified value of the sum is again divided by the dynamic value to produce the final value.

From the final value the value after decimal up to first two decimal places is extracted, this indicates the position after which Mixed array insertion is done.

Several operations done by exploiting the dynamic value insures the secrecy as well as the non repeatable property of the algorithm during its repetitive usage.

4.2. Fundamental steps associated with the D.G.L.P.G. technique

The value of the attribute $k5$ is assigned in the equation (1) and unique value is generated.

From the generated unique value the value after decimal from the 4^{th} to the 6^{th} decimal place is extracted and is set as priority value of the actual node.

The above process is followed for generating priority values for each individual node by successively increasing the value of the attribute $k5$ by 1 after each turn of priority value generation.

4.3. Fundamental steps associated with the foundation of key insertion position

The key insertion position determinant is determined by adding the extreme Mixed array position that is 99, the extreme password length that is 64, the extreme quantity of false values to be inserted that is 32, which is 195.

Jumping one value after 195 we have selected 197 as a determinant.

The key insertion position is the additional result of the determinant and the last digit value of the two digit value of the attribute $k4$, which can vary in the range from 197 (197+0) to 206 (197+9). As a key actual length of the password will be given.

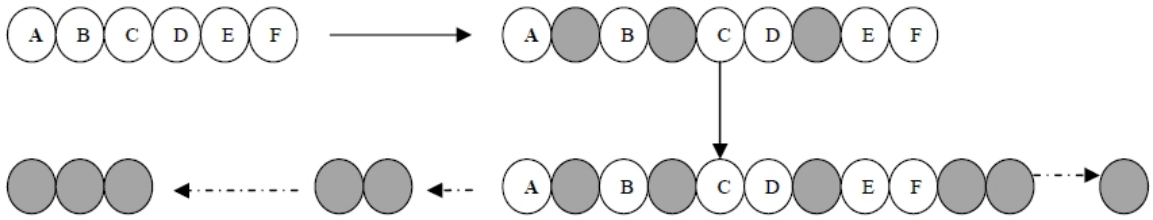

Figure 1. Representing the Encryption technique where dynamic password inserted is "ABCDEF"

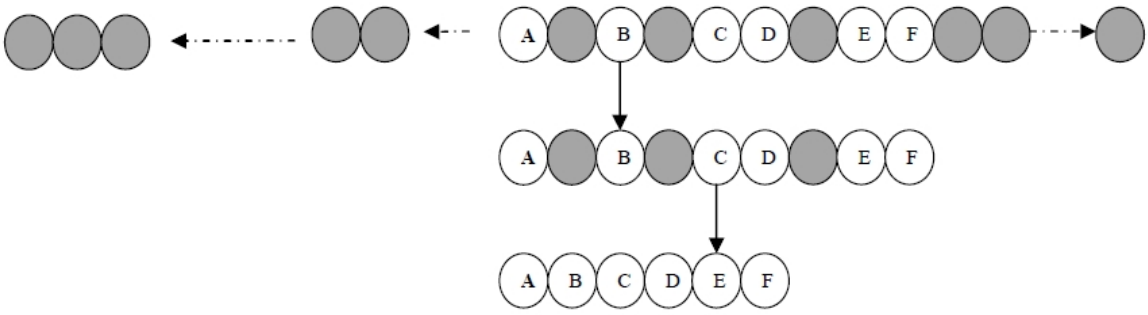

Figure 2. Representing the Decryption technique and retrieval of dynamic password "ABCDEF"

5. PRESENTED ALGORITHMS

Presented algorithm is illustrated below in two parts as encryption and decryption algorithms.

5.1. Encryption algorithm

Dynamic password encryption algorithm is depicted below through the following steps as

Step 1: Take the length of the password (l) and the password from the user and convert it into the ascii form.

Step 2: Generate the Finalpwd array position (F) after which Mixed array will be inserted.

Step 3: [Initialization] Set $i = 1$

Step 4: Repeat Step 5 and 6 while $i \leq l$

Step 5: Create priority for each individual actual password node using D.G.L.P.G. technique and store it in the Priority array.

Step 6: Set $i = i + 1$

Step 7: End

Step 8: Sort the Priority array and arrange the Prioritypositon array accordingly.

Step 9: [Initialization] Set $i = 1$

Step 10: Repeat Step 11 and 12 while $i \leq l/2$

Step 11: Generate false node insertion position as per value indicated by the Prioritypositon array and F and then store it in the False array.

Step 12: Set $i = i + 1$

Step 13: End

Step 14: Set $q = l - l/2$

Step 15: [Initialization] Set $i = 1$

Step 16: Repeat Step 17 and 18 while $i \leq q$

Step 17: Generate actual node insertion position as per value indicated by the Prioritypositon array and F and then store it in the Actual array.

Step 18: Set $i = i + 1$

Step 19: End

Step 20: [Initialization] Set $i = 1$

Step 21: Repeat Step 22 and 23 while $i \leq l/2$

Step 22: Insert false value at the position indicated by False array in the Finalpwd array by maintaining the Shifting property of the algorithm.

Step 23: Set $i = i + 1$

Step 24: End

Step 25: Set $q = l - l/2$

Step 26: [Initialization] Set $i = 1$

Step 27: Repeat Step 28 and 29 while $i \leq q$

Step 28: Insert actual node at the position indicated by the Actual array by maintaining the Shifting property of the algorithm.

Step 29: Set $i = i + 1$

Step 30: End

Step 31: [Initialization] Set $i = 1$

Step 32: Repeat Step 33 and 34 while $i \leq F$
Step 33: Generate random values at the position indicated by i.
Step 34: Set $i = i + 1$
Step 35: End
Step 36: Set $F' = F + l + l/2$
Step 37: [Initialization] Set $i = F' + 1$
Step 38: Repeat Step 39 and 40 while $i \leq 256$
Step 39: Generate random values at the position indicated by i.
Step 40: Set $i = i + 1$
Step 41: End
Step 42: Insert the actual length of the password as a key

5.2. Decryption algorithm

Dynamic password decryption algorithm is depicted below through the following steps as:

Step 1: Find the key insertion position (k)
Step 2: Extract the key from k
Step 3: Set length of password (l) = key
Step 4: Generate the Finalpwd array position (F) after which mixed array is inserted.
Step 5: Extract the Mixed array from the Finalpwd array.
Step 6: [Initialization] Set $i = 1$
Step 7: Repeat Step 8 and 9 while $i \leq l$
Step 8: Create priority for each individual actual password node using D.G.L.P.G. technique and store it in the Priority array.
Step 9: Set $i = i + 1$
Step 10: End
Step 11: Sort the Priority array and arrange the Priorityposition array accordingly.
Step 12: [Initialization] Set $i = 1$
Step 13: Repeat Step 14 and 15 while $i \leq l/2$
Step 14: Generate false node insertion position as per value indicated by the Prioritypposition array and F and then store it in the False array.
Step 15: Set $i = i + 1$
Step 16: End
Step 17: Set $q = l - l/2$
Step 18: [Initialization] Set $i = 1$
Step 19: Repeat Step 20 and 21 while $i \leq q$
Step 20: Generate actual node insertion position as per value indicated by the Prioritypposition array and F and then store it in the Actual array.
Step 21: Set $i = i + 1$
Step 22: End
Step 23: Set $F' = F + l + l/2$
Step 24: [Initialization] Set $i = F + 1$
Step 25: Repeat Step 26 and 27 while $i \leq F'$
Step 26: Insert nonzero value in the Retrieve array at the position indicated by i.
Step 27: Set $i = i + 1$

Step 28: End

Step 29: [Initialization] Set $i = 1$

Step 30: Repeat Step 31 and 32 while $i \leq l/2$

Step 31: Insert zero value in the Retrieve array at the position indicated by False array by maintaining the Shifting property of the algorithm.

Step 32: Set $i = i + 1$

Step 33: End

Step 34: [Initialization] Set $i = F + 1$

Step 35: Repeat Step 36 and 37 while $i \leq F'$

Step 36: Extract the node value as actual node value from the mixed array at the indices where Retrieve array value is a nonzero value and convert the corresponding ascii value to the corresponding symbol.

Step 37: Set $i = i + 1$

Step 38: End

6. EXPERIMENTAL RESULT OF THE PROPOSED ALGORITHMS

The experimental result of the presented algorithm is examined using Intel ®Core$^{TM}i3$ processor. Here the supported system is a 64 bit machine with 4GB RAM capability. The programming language which is selected for implementing the algorithm is "C" and the compiler used for this purpose is Turbo 'C' compiler. The experimental results are presented below in the tabular form here the first column represents the true length of the dynamic password, the second column and the third column represents the encryption and the decryption time respectively and the last column represents the total time taken for encryption and decryption.

7. ANALYSIS OF THE REAL WORLD APPLICATION OF THE PROPOSED TECHNIQUE

The proposed technique is a unique and revolutionary attempt, due to its way of generating, encrypting dynamic password/OTP as well as its way of creating secure session which is quiet uncommon to former approaches. Hence we have considered the most common application field that is financial systems where use of OTP based authentication is a daily routine tasks to illustrate the necessity of the proffered algorithm [11, 24]. Man-in-the-Middle attack has become a buzzword now days. It can be conducted in several manners that mean either the intruder can imitates him/her as the user who requests for financial service or intruder can imitates him/her as the financial body that provides financial services. The risk assessment is done for both of these previously mentioned cases. Proposed technique shows its concern mainly for network security. As the implementation of the proposed technique should be done on the 3-way Client initiated authentication principle so, it is a time consuming process. But when a big financial deal has to be done of heavy amount then a different approach, dissimilar to one that is taken for major small financial deals is needed to be taken towards designing a secure system. In this kind of perilous situation the robustness of the security system dominates the delay factor associated with security system that means if high level secrecy is required then we must have to accept a bit longer delays.

Table1. Encryption time, decryption time and total time taken for various dynamic password lengths

Length of the dynamic password	Time taken for Encryption(Seconds)	Time taken for Decryption (Seconds)	Total Time
4	0.015653	0.012711	0.028364
6	0.018242	0.011459	0.029701
8	0.016758	0.014951	0.031709
11	0.018773	0.020763	0.039536
16	0.02953	0.032408	0.061938
17	0.022975	0.035633	0.058608
19	0.033665	0.02128	0.054945
22	0.036281	0.036979	0.07326
25	0.040555	0.041863	0.082418
27	0.044014	0.010931	0.054945
29	0.042888	0.02732	0.070208
40	0.051282	0.058608	0.10989
50	0.069801	0.040089	0.10989
64	0.076313	0.070207	0.14652

For risk assessment the general condition where the financial system as Bank's Server generates the OTP for a particular client/user requesting financial service is considered.

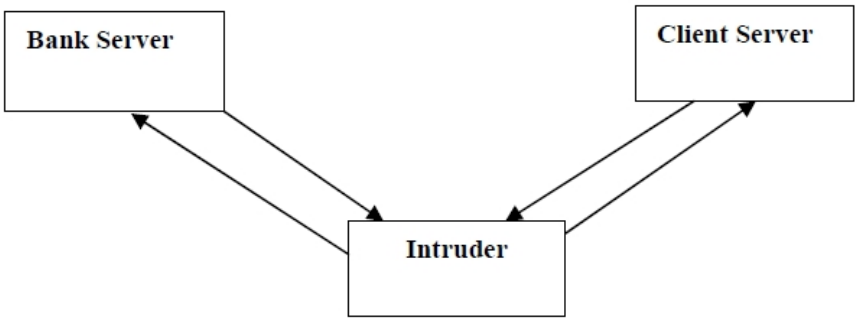

Figure 3. Representing the Intruders control over the session

Through MiM attacks an intruder can easily control the session between the valid communicators.

Intruder acts as Bank Server to Client: Phishing attack can be used to redirect the Client to intruder's web site and all confidential information that user name and password of the Client can be stolen. In this scenario it is assumed that intruder is able to retrieve the actual static password even if it is encrypted. Then based on the previous observation of kind of OTP cipher used to be generated by the Bank server one stolen false encrypted OTP cipher is sent to the Client. Client extracts the False OTP and sends it back to the intruder

assuming him / her legitimate. Now intruder can perform chosen plain text analysis attack or cipher text only analysis attack to find out the cryptographic logic.

Intruder acts as Client: Now intruder knows static password as well as cryptographic logic of OTP encryption. Now intruder acts as Client authenticates himself and whatever encrypted OTP is sent from the Bank server side he/ she is able to find out the correct OTP and completely validates the transaction. Hence as a Client it can request bank for illegal transactions from actual Client's account.

The proposed technique can be utilized here to form 3-way Client initiated authentication system. Where Client as per his choice decides the OTP then encrypted OTP is supposed to be decrypted at the bank server end. Again as an acknowledgement from Bank the same OTP is encrypted with same proposed algorithm with different attributes that changes due to even very minor change in the real time system. The encrypted OTP is again decrypted at Client side and this assures Client that it is communicating with the Bank only. But for the Bank to get ensure where it is the actual Client or not again Client will have to send the OTP which is again encrypted following the same process as mentioned before and again Bank decrypts the OTP to validate the Client and to be assured that the communicating party on the other side is Client and not the intruder. And lastly from Bank server side a positive response of "Successful Session" is sent. In this way 3 times identification is done so it is time consuming but the level of security is high and is required to authenticate that communication is going on between both legal parties and no chances are given to intruder to interrupt the communication by making any false connection.

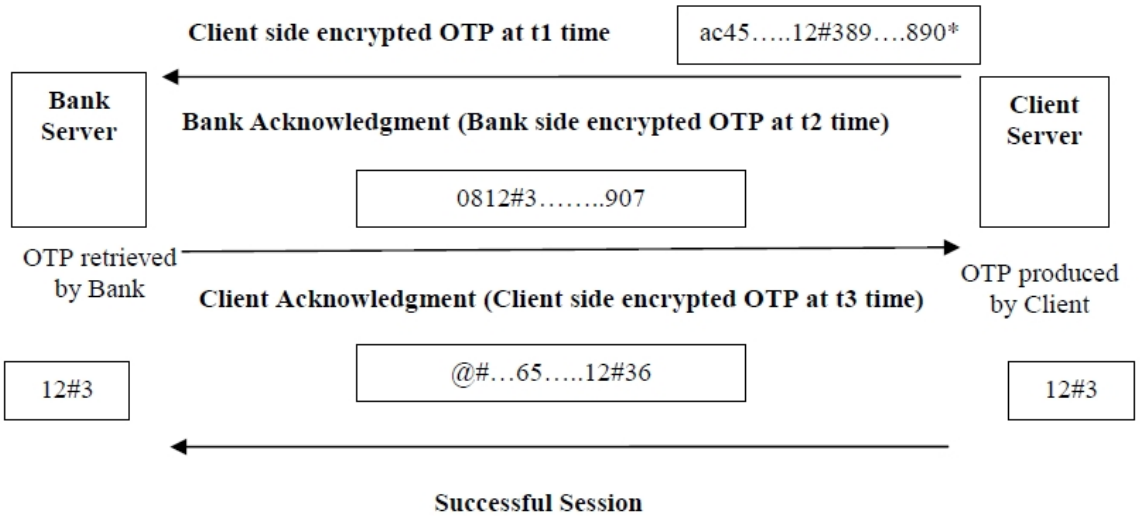

Figure 4. Representing the application of proposed algorithm in Financial System

Each time OTP is encrypted using proposed algorithm using the parameter selected from the current date and time system whose value changes during that specific period of time, diagrammatic representation presented above illustrates the logic required for actual implementation in financial system. Additionally during generation of Mixed array insertion position the factor named as "user counter factor": that is which number of user is requesting

if used which is incremented per user and is initialized to zero after particular constant value is reached, then for multiple user at same time variations in cipher can be achieved. Adding an extra layer of security is always preferable when a robust security system has to be designed. Implementation of the proposed algorithm eliminates the threat of MiM attack whether intruder imitates him/her as Client or bank, will fail to get any control over the session.

Intruder acts as Bank Server to Client: In this case intruder will fail to decrypt the encrypted OTP and if intruder sends a false acknowledgment then the Client will get a wrong OTP acknowledgement and from the Client side session will be broken.

Intruder acts as Client: In this case even if the intruder sends a false OTP with matching length of the actual encrypted key, then Bank server will decrypt it and hence will get a false OTP, and then it will again encrypt the same false extracted OTP with the encryption algorithm and will send it back to the intruder. But the intruder will fail to decrypt the acknowledgement and hence will fail to send any further acknowledgement or even If the intruder sends a further false acknowledgement, then at the time of decryption at the Bank server side the presence of intruder will be detected as the extracted OTP at the Bank side this time differs from the previously obtained false OTP from Client. Hence session will be broken.

The proposed algorithm can also fit itself for other diverse application arenas as Nuclear Power Plant Security system, as a platform for critical e-commerce or m-commerce transaction requirements, to protect critical servers, to transfer valuable data in clouds. But the certainty of any technique appeals its implementation in the physical world. Moreover there is an always a scope of betterment, presented technique can be taken as a basis for developing more robust security system with additional features.

8. CONCLUSIONS

Sustainability is one of the most demanding as well as challenging goal of most of the competitive organizations whether it is government or non government and active in specific or diverged sections. In today's technical drift this kind of ambitious goals can never be achieved without technical support. This kind of technical support will be evaluated as incomplete without the assistance of security mechanisms. Intensified view of required security mechanism gives the reason to think in broader way while dealing with theses sensitive issues. These issues are sensitive because they are related to those data and processing systems which produce information of high significance. Therefore an integrated approach is necessary to develop a robust security system. This kind of unified technique is combination of static and dynamic passwords. Presented paper which is focused towards the dynamic passwords, is an effective step in distributing the entire burden of ensuring security only on static passwords. A diverged method reduces the complications related to static password based security mechanisms that puts restrictions on users to choose complex kind of static passwords but in common practices users always tends to select the easier and memorable one. Reduction of the load on static password encryption mechanisms should not be misinterpreted as dynamic password encryption mechanisms will be more critical ones for the user. Considering this fact in mind a keen study is done over the current dynamic password encryption mechanisms. It is observed that at the cost of high time complexity,

increased dependency on several algorithmic parameters, increased complexities in terms of implementation a supreme security is promised. But an optimal way is the most suitable way to deal with such kind of changeable situations. The proffered algorithm suggests an extremely secure way. It is very simple to implement however time synchronization is an important factor. It is user friendly in nature, it allows users to select a dynamic password of their own choice even single character long however in general at least four characters long dynamic password should be selected. Its excellent brute force resistance capability makes it able to provide a contiguous resistibility for any length of dynamic password with 256 characters long cipher. With its perfect dynamic feature it is not at all dependent on any static entity, hence no database storage and maintenance is required. The proffered algorithm has obtained very low space complexity and time complexity which is $O(\log n)$ where n is the length of the password. The actual implementation could take bit more time in session generation, due to the 3-way Client initiated authentication principle. But it is necessary for both legal communicating parties to ensure the legitimate presence of each other. As an integrated security system it can be implemented in a wide range of application fields as: Mobile or Internet Banking, Nuclear power plant security system etc.

REFERENCES

[1] M. H. Ali, "Voiced 3d password authentication," *International Institute for Science, Technology and Education*, vol. 4, no. 6, pp. 87–91, 2014.

[2] H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell, "Secure graphical one time password (gotpass): An empirical study," *Information Security Journal: A Global Perspective*, vol. 24, no. 4-6, pp. 207–220, 2015.

[3] S. Bhardwaj, V. Gandhi, V. Yadav, and L. Poddar, "New era of authentication: 3-d password," *International Journal of Science, Engineering and Technology Research*, vol. 1, no. 5, pp. 23–27, 2012.

[4] F. Cheng, "Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm," *Mobile Networks and Applications*, vol. 16, no. 3, pp. 304–336, 2011.

[5] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "Otp-based two-factor authentication using mobile phones," in *Information Technology: New Generations (ITNG), 2011 Eighth International Conference on*. IEEE, 2011, pp. 327–331.

[6] P. K. Gopinadhan and B. A. Naremparambil, "Passaction: A new user authentication strategy based on 3d virtual environment," *International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN 2249–9555*, vol. 2, no. 2, pp. 282–285, 2012.

[7] C. Hoffman, "Brute- force attacks explained: How all encryption is vulnerable [online] available:," *http://www.howtogeek.com/166832/*, 2013.

[8] W.-B. Hsieh and J.-S. Leu, "Design of a time and location based one-time password authentication scheme," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*. IEEE, 2011, pp. 201–206.

[9] C.-Y. Huang, S.-P. Ma, and K.-T. Chen, "Using one-time passwords to prevent password phishing attacks," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1292–1301, 2011.

[10] A. A. Khatpe, S. T. Patil, A. D. More, D. V. Waghmare, and A. S. Shitole, "3d login for more secure authentication," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 2, pp. 2992–3000, 2014.

[11] Y. Ku, O. Choi, K. Kim, T. Shon, M. Hong, H. Yeh, and J.-H. Kim, "Two-factor authentication system based on extended otp mechanism," *International Journal of Computer Mathematics*, vol. 90, no. 12, pp. 2515–2529, 2013.

[12] S. Lee and K. M. Sivalingam, "An efficient one-time password authentication scheme using a smart card," *International Journal of Security and Networks*, vol. 4, no. 3, pp. 145–152, 2009.

[13] H. Parmar, N. Nainan, and S. Thaseen, "Generation of secure one-time password based on image authentication," *Journal of Computer Science and Information Technology*, vol. 7, pp. 195–206, 2012.

[14] I. Paul, "Lenovo preinstalls man-in-the-middle adware that hijacks https traffic on new pcs, pcworld [online] available:," *http://www.pcworld.com/article/2886357/lenovo-preinstalls-man-in-the-middle-adware-that-hijacks-https-traffic-on-new-pcs.html*, 2015.

[15] G. J. Rajguru and et al., "Secure authentication with 3d password," *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 5, pp. 68–75, 2014.

[16] K. Ramesh and S. Ramesh, "Implementing one time password based security mechanism for securing personal health records in cloud," in *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on.* IEEE, 2014, pp. 968–972.

[17] D. Raval and A. Shukla, "Security using 3d password," *International Journal of Computer Applications*, vol. 120, no. 7, 2015.

[18] M. R.Sujatha and M.L.Suchithra, "Score level fusion based otp generation using biometric ecc," *International Journal of Advanced Engineering Technology*, vol. 7, no. 2, pp. 1030–1035, 2016.

[19] V. Shivraj, M. Rajan, M. Singh, and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for internet of things (iot)," in *Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on.* IEEE, 2015, pp. 1–6.

[20] A. D. Sumathy and et al., "Otp encryption techniques in mobiles for authentication and transaction security," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 10, pp. 6192–6201, 2014.

[21] N. Vishwakarma and K. Gangrade, "Secure image based one time password," *International Journal of Science and Research*, vol. 5, no. 11, pp. 680–683, 2016.

[22] P. Wood and et al., "Internet security threat report," *Symantec Co.*, vol. 17, 2012.

[23] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "Cloud authentication based on anonymous one-time password," in *Ubiquitous Information Technologies and Applications.* Springer, 2013, pp. 423–431.

[24] L. Yinxiang, X. Li, L. Zhong, and Y. Jing, "Research on the s/key one-time password authentication system and its application in banking and financial systems," in *Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on.* IEEE, 2010, pp. 172–175.

Received on September 29 - 2016
Revised on May 12 - 2017