Two Factor Authentications Using One Time Random Password for Secure Online Transaction

G.Umamaheswari
PG Scholar (M.Phil-CS), Selvamm Art Science College (Autonomous), Namakkal, Tamilnadu, India
Uma.hkrh@gmail.com
Dr.A.Kangaiammal
Assistant Professor (CS), Governtment Arts College, Salem,Tamilnadu, India
Indurath2002@yahoo.co.in
K.K.Kavitha
Assistant Professor (CS), Selvamm Arts and Science College (Autonomous), Namakkal, Tamilnadu, India.

ABSTRACT

The concepts of secure transactions are essential for almost all online transaction. Generally such methodologies were adapted in recent days using one time password. The one time password is a random password generated by the server send to the user for their person authentication access. In contract with the traditional approach the work addresses the concept of two factor authentication for accessing and approving the one time password by the legitimate user. This works on all platforms and applications that are either may be online processed transaction done via system or electronic gadgets. This work will add additional secure measure despite the security poised by the one-time password. Also the work neglects the processing of automatic server processing by implementing the concept of self-reliable code that is generally termed as capcha code.

Keywords - **OTP, Secure transactions, TWO factor authentication, Self-reliable code**

Date of Submission: January 6, 2015 Date of Acceptance: February 10, 2015

I. INTRODUCTION

The concepts of OTP[1] using two factor semi-automatic authentications messaging via secure channels are used widely in network mechanism. These methods are used in online secure transaction especially in the case of payment process. OTP can be achieved either via SMS or any digital messaging service for providing consistent service. The OTP messages will be duplicated as times when the medium lays inaccessible leads to duplicated services. The fore said mechanism is implemented in our work by avoiding duplication by maintaining medium information along with acknowledgement. The service will commit once for a while it accomplish successes fully.

The problem with two factor authentication also has few pitfalls arises in the form of following outcomes

(i) Sending SMS to users
(ii) Delay messaging in sending/receiving
(iii) Extending boundary
(iv) Secure transaction

Sending SMS to users: While sending the OTP to the user, the concern authority or the providers will send SMS in the form of OTP to the user electronic medium or gadgets for getting their instant approval for all the transaction.This involves two way communications for sending the SMS and receiving the acknowledgment. The receiving SMS will be charges depending on the provider's constraint. If sending the SMS falls within the scope of the provider's constraint then it will also be consider as the criteria for either sending or receiving the SMS.

Delay messaging in sending/receiving: The receiving and sending SMS will be left unnoticed when the charge is taken by the provider and the message is not delivered. This is because of the huge network traffic and that leads to delay. Generally the delay arises in both ends(sending/receiving). In order to avoid such factor affecting the transaction the delay is measured and the alternative way has been chosen to resend the code that expire the previous message send via the same portal.

Extending boundary: Generally the term boundary meant here as the limitation for sending and receiving SMS between the system and the user for making the transactions. Innetwork term it is referred as roaming. When the boundary of the network is increased, the criteria for making the transaction will vary and tend to change accordingly. Generally the delay in the network will increase when the distance increase as these two terms are directly proportional.

Secure transaction: The concept of security is indulged for almost every online transaction. Generally such terms was checked with the online password generated by the user themselves. As the password hint is very narrow to be hacked the concept is extended further with random password check. Even this approach is viable to attack as the server is tent to produced random password which can also be hacked. To overcome this, concept of One-time password is

introduced by which both the ends are checked for liability before making the transaction.
In this paper all the above mentioned criteria are addressed with the concept of two factor authentication which will be explained in detailed by the Section 4 of this work.

II. LITERATURE SURVEY

Leslie Lamport[3] holds the ownership for introducing the concept of OTP which address the principles of OTP by which two extreme ends users are authenticated simultaneously while making transaction. The main objective of OTP will avoid resending of the message when the previous message was left undelivered. Such mechanism is so called as Reply attack [5] which will increase the vulnerability of the transaction.

N. Haller [2] uses the concept of S/Key for sending OTP initiated by a single seed. A seed is the systematic approach of the single system that either generates OTP or authenticates it. The usage of hash function applied for all the transaction made by the seed or the system. The hash function also addresses the length of the password generated for valid authentication system.

The hash function used in the systematic approach of N.Hallerrepresents the length of the hash key represented as

$$h(s) = h^1(s), h^2(s), \dots \dots h^{n-1}(s), h^n(s) \quad (1)$$

In order to send the OTP along with the hash function [6] the formulae is redefined as

$$h(s) = h(s) + OTP(s) \quad (2)$$

The above equation gives the length of the hash key generated by the approach shown the N.Haller work. To generate OTP along with hash function eqn (2) is used.

To check both the system and user the eqn (3) is used

$$h(s)^t = h(s)^N + OTP(s)^{t+1} \quad (3)$$

where 't' is the system authentication factor t-1 is the factor for sending the OTP and t+1 is the system increment.

K. Bicakci and N. Baykal [4], focus on hash function along with its length that sends one-time password in infinite way of access. The protocol proposes RSA algorithm with the classification of private key and public key.

$$h(s + e) = h(s) + OTP(s) \quad (4)$$
$$h(s) = h(s + d) + OTP(s) \quad (5)$$

The classification of e and d, are encryption and decryption.

III. EXISTING WORK

The existing work addresses the concept of OTP using hash function with valid chain. It also addresses the encryption [8] along with hash function chain and the decryption works on the reverse factor with the same hash function and its length.

To invoke security in the hash function that can be either hardware or software, a token is generated along with the system (seed). The timer concept of OTP is done with this concept and using the token the secure id is generated.

In order to avoid public key cryptography, the concept of random password is generated and it leads to OTP generation. Hence there will be system will be generated and there will be another system which evaluated or authenticates it.
The combination of OTP will be framed using system authentication S(A) and system generation S(G). The user login and authentication will works on the following points
(1). User login process for making transaction
(2). User was identified by the server
(3). User corresponding OTP authentication process
(4). User authentication process and server authentication check
Figure (1) represents OTP generation using hash function using the above steps mentioned in the frame work.

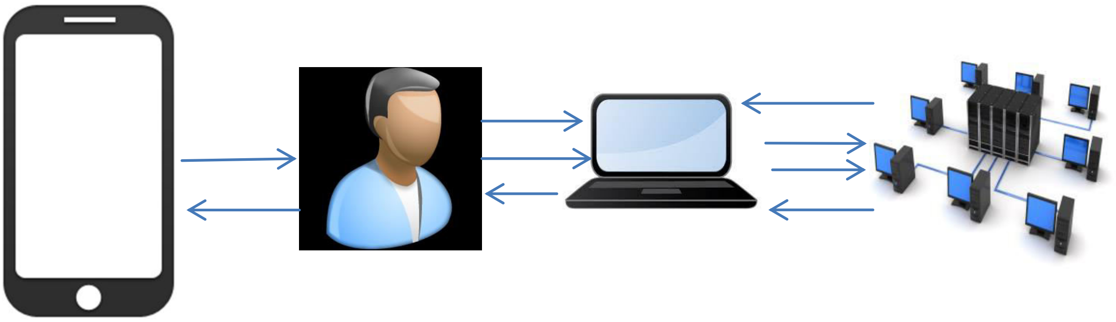
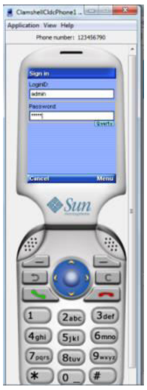


Fig 1: User authentication for OTP generation using hash functions

IV. PROPOSED WORK



Phone number: 123456790

Sign in

LoginID: admin

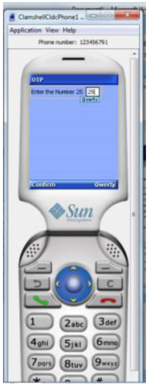
Password: *****

Fig 2: User login process

This is the first phase of the process. The user is authenticated with username and password. The login process is classified based on the user login mode. Two modes are adapted in the process. First mode is the user mode and followed by the admin mode.

The user mode is the seed mode by which both the user and the system are identified and the seed is set. The admin mode will guide the authentication process including user and the system for further access. The admin will provide access rights to the user so as their system.

In this phase, OTP is generated with the default digit entry made to continue the process. Such process will avoid zombie attack and ensure the human is working with the digital media and in extend it works as a capcha based approach to authenticate the process.



Phone number: 123456791

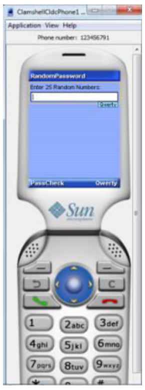
OTP

Enter the Number 25: 25

Fig 3: OTP generation

The Fig 4 will make random hash function chain generation. This will initiate the process once after successful user based authentication is done by the system.

The Fig 5 generates OTP generation. This will be[1] followed by OTP generation where all the three process were combined to make successful authentication.



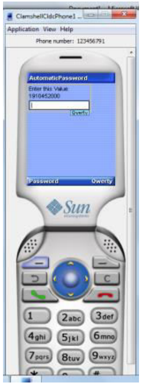
Phone number: 123456791

RandomPassword

Enter 25 Random Numbers:

The Fig 6 shows the successful login process with valid Random number generation in phase 1 and OTP generation in phase 2 and hence forth the technique is referred as two factor authentications.

Fig 4: Hash chain generation

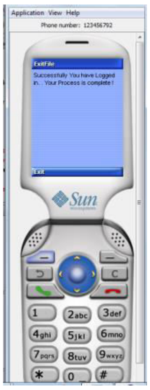


Phone number: 123456791

AutomaticPassword

Enter this Value
1910452000

Fig 5: Random OTP generation



Phone number: 123456792

ExitFile

Successfully You have Logged in... Your Process is complete !

Fig 6: Login process success with OTP

V. CONCLUSION

The results shown in this work, implements two factor authentication and to continue further the concept of hash chain function is also included in the process. Future works reflects on public key cryptography for generating the code as this work address only the basis of OTP generation using hash function and that depends on seed or system classification.

REFERENCE

[1] Faisal, Saqib, et al. "Facile (Triazolyl) methylation of MACOS-derived BenzofusedSultams Utilizing ROMP-derived OTP Reagents." *ACS combinatorial science 14.4 (2012): 268-272.*

[2] N. Haller, "The S/KEY One–Time Password System. In: *Proceedingsof the ISOC Symposium on Network and Distributed SystemSecurity", 1994, pp. 151-157*

[3] L. Lamport, "Password Authentication with Insecure Communication",*In: Comm. ACM, vol. 24, No 11, 1981, pp. 770-772.*

[4] K. Bicakci N. Baykal, "Infinite length hash chains and theirapplications" In: *Proceedings of 1st IEEE Int. Workshops on EnablingTechnologies: Infrastructure for Collaborating Enterprises WETICE'02,2002, pp. 57-61.*

[5] Goyal, Priyanka, SahilBatra, and Ajit Singh. *"A literature review of security attack in mobileadhocnetworks." International Journal of Computer Applications 9.12 (2010): 11-15.*

[6] Goldwasser, Shafi, Silvio Micali, and Ronald L. Rivest. *"A digital signature scheme secure against adaptive chosen-message attacks." SIAM Journal on Computing 17.2 (1988): 281-308.*

[7] SUN, Ke-qiang, Jia-yong LIU, and Guang-hua DING. *"An OTP Scheme Based on Hash Function and Symmetry Encryption [J]." Information and Electronic Engineering 6 (2007): 012.*

Author's Details:

G.Umamaheswari, who is a student in Department of Computer Science,Selvamm Arts and Science College (Autonomous)

Dr.A.Kangaiammal received both B.Com. and MCA from Bharathidasan University, Trichy in 1993 and 1996, respectively. M.Phil. from ManonmaniamSundaranar University, Tirunelveli in 2001. Ph.D. in Computer Applications from the University of Madras in 2009. Her research interest includes Data Mining, Mobile Computing, Web Mining, E-Learning, Content Development, Instructional Design and Curriculum Development. She is an Assistant Professor of Computer Applications in Government Arts College (Autonomous), Salem-7. She has morethan 15 years of teaching and research experience. She is a life memberof ISTE and SETRAD. She is also a member in ACM.

Ms.K.K.Kavitha, MCA,M.Phil, works as Assistant Professor in Selvamm Arts and Science College, Namakkal , India. Her fields of interest areData Mining, Softcomputing. She has 12 years' experience in teaching.