International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8595-8601

An Approach to Implement Secure User Authentication Scheme using Secret Values extracted from Private Information and Unique Biometric Images of User directed by Randomize Numeric and Image based OTP

Ramkrishna Das[1], Aditi Chakraborty[2], Santosh Nandi [3] and Saurabh Dutta[4]

[1]Department of Computer Applications, Haldia Institute of Technology, Haldia-721602, Purba Medinipur, West Bengal, India.
[2,3]Department of Computer Science, Panskura Banamali College, Panskura-721152 Paschim Medinipur, West Bengal, India.
[4]Department of Computer Applications, Dr Bidhan. Chandra. Roy. Engineering College, Durgapur-713206, Burdwan, West Bengal, India.
ORCIDs: [1]0000-0003-2354-9904, [2]0000-0001-9654-4552, [3]0000-0001-6822-1158, [4]0000-0001-5892-0094

Abstract

Proposed system introduces a numeric OTP (one time password) based authentication system where a secured value extracted from user private information(user id, password and security questions) and unique biometric image directed by the OTP is used for authentication rather than using the direct OTP value. Server randomly selects the position of character and number of block of pixels from randomly selected modified private information of user and user biometric images. Finally we combine those positions and block number of pixel and generate intermediate OTP. Final OTP will be generated from intermediate OTP using digit repositioning scheme which will be shared to user. User extracted and formulates secured values from private information and biometric image directed by the numeric value of intermediate OTP. That secured value is used for authentication. Random selection of characters and pixels from randomly selected user information and biometric image, distribution of OTPs in multiple communication mode, formation of separate OTPs for distribution (final OTP) and user authentication (intermediate OTP), extraction and use of secured values from user private information and biometric image for authentication directed by intermediate OTP impose a great security to the proposed system.

Keywords: Numeric OTP, OTP directed Value Extraction, Random Selection, Biometric Image, Character Repositioning Scheme.

INTRODUCTION

Traditional numeric One Time Password (OTP) is not so much secured as distribution of OTP is done through public communication channel[8, 9] . So we have proposed an OTP system where a secured value extracted as per the numeric value of the OTP is used for authentication rather than using the direct OTP value. Secured value is extracted from user private information (user id, password and security questions) and unique biometric image directed by numeric value of the OTP.

Background Study

Yun Huang, Zheng Huang, Haoran Zhao and Xuejia Lai proposed an OTP method that generates a unique passcode based on both time stamps and sequence numbers [1]. Neha Vishwakarma and Kopal Gangrade introduced an approach that system uses random image and text based OTP generation with SHA-512 algorithm and again encryption by using ECC to develop OTP [2]. Ananthi Sheshasaayee and D. Sumathy define a system where OTP is transformed using a lightweight cryptography and hide the cipher text using text steganography and send the stego text as SMS to user mobile. Personal Identification Number (PIN) supplied by the bank to user during registration is used for ciphering. PIN is needed to decrypt the OTP [3]. WenBin Hsieh and Jenq-Shiou Leu proposed a novel authentication scheme which exploits volatile One-Time Passwords (OTPs) based on the time and location information of the mobile device to securely authenticate users while accessing Internet services[4]. Safa Hamdare, Varsha Nagpurkar and Jayashri Mittal introduced a mechanism where OTP is combined with the secure key and is then passed through RSA algorithm to generate transaction password. The activities are carried out both in server and user side so distribution is not needed over public network [5]. Navpreet Kaur , Mandeep Devgan and Shashi Bhushan proposed a model which involves seed exchange, a software-based token via Transport Layer Security(TLS) tunnel which is used to generate online one time passwords. Authentication occurs through the verification of OTP generated at server and

OTP generated from the shared seed value on the android mobile phone of user [6]. Tamanna Saini introduced a method of generating OTP by using genetic algorithm with elliptic curve cryptography [7].

Objective of the Article

Proposed system introduced a numeric OTP based authentication system where direct OTP value is not been used for authentication rather than secured value extracted from user private information(user id, password and security questions) and unique biometric image directed by the OTP is used for authentication

Multiple layers of securities are being imposed in the proposed system. User id and password based authentication, random selection of characters, pixels from randomly selected text and biometric image, distribution of OTPs in multiple communication mode, formation of separate OTPs for distribution (final OTP) and user authentication (intermediate OTP), extraction and use of secured values from user private information for authentication directed by intermediate OTP impose a great security to the proposed system.

Structure of the Article

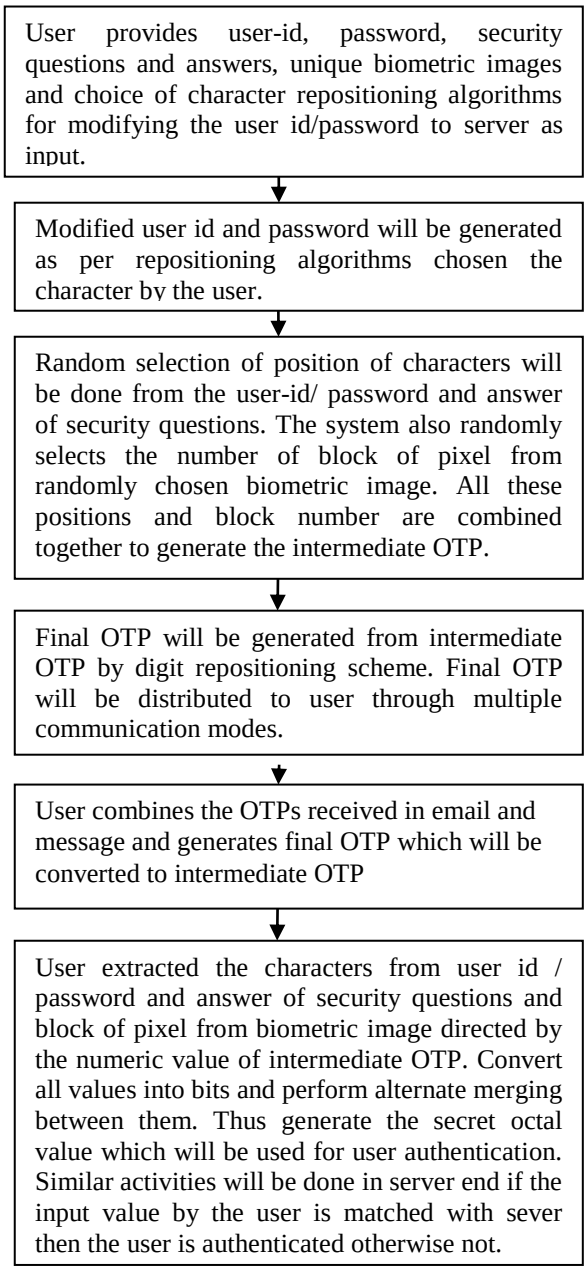
In this paper, Section-II discusses preliminaries. Section-III describes the overall procedure. Section-IV, Section-V and Section-VI represents formation of OTP at server, distribution of OTP, extraction of OTP at user end and authentication respectively. Experimental results are described in section-VII. Section-VIII shows the comparison with existing OTP system and section-IX draws conclusions.

PRELIMINARIES

One Time Password

A one-time password (OTP) is a numeric or alphanumeric string of characters which is generated by a server automatically. OTP authenticates the user for transaction or session. OTPs may be used as additional layer of security. OTPs are not vulnerable to reply attack and have a great advantage on static password. OTPs are valid for only one login session or transaction [8].

Overall Procedure



Formation of OTP at Server End

Algorithm for taking user inputs to server

User provides user-id, password, unique biometric images, security questions and answers and choice of character repositioning algorithms for modifying the user id/password to server as input.

Algorithm for Character Repositioning Schemes for modifying User-Id/Password

The positions of the characters of the user-id/ password are being re-positioned separately by using one of the character repositioning algorithms chosen by the user. The algorithms are defined below.

PRONE (Positional Reverse Odd Normal Even)
Store each digits in an array pro[]. Fetch and reverse the odd position digit's value and store them in array pro_f[]. Even position's digits are stored to array pro_f[] without any changes.

PRENO (Positional Reverse Even Normal Odd)
Store each digits value in an array pre[]. Fetch and reverse the even position digit's value and store them in array pre_f[]. Odd position digits are stored to array pre_f[] without any changes.

CRENO (Continuous Reverse Even Normal Odd)
Store each digits value in an array cre[]. Fetch and reverse the even position digit's value and store them in array cre_f[] continuously. Odd position digit's are stored to array cre_f[] continuously without any changes.

CRONE (Continuous Reverse Odd Normal Even)
Store each digits value in an array cro[].Fetch and reverse the odd position digit's values and store them in array cro_f[] continuously. Even position digit's are stored to array cro_f[] continuously without any changes.

Algorithm for Generating Numeric Intermediate OTP

Step I: System randomly selects the positions of characters from randomly selected user-id or password and answers of the security questions. System also randomly selects the block of pixel from randomly selected biometric image. All these positions and block number are combined together to generate the intermediate OTP. The structure of the intermediate OTP is represented in figure 1.

Block-1		**Block-2**	
Position of character randomly selected from user-id /password		**Position of character randomly selected from answers of security questions**	
Code to select user-id / password (1/2)	Value for randomly selected N^{th} character	Code to select answer of security questions (1/2/3)	Value for randomly selected N^{th} character

Block-3		
Position of block number of pixels randomly selected from biometric images of user.		
Code to select biometric image randomly (1/2/3)	Code to select Pixel randomly	Code to select block of pixel randomly (1/2/3/4)

Figure 1: Structure of the intermediate OTP

Algorithm for Generating Numeric Final OTP

Final OTP will be generated from intermediate OTP by using digit repositioning scheme. We fetch single digit position wise from each of the three blocks of intermediate OTP and store them into an array called FINAL_OTP[] in each iteration. All the digits present in three blocks of the intermediate OTP will be fetched in that manner and stored into the array FINAL_OTP[]. Thus generate the final OTP.

Algorithm for main() function

Step I: Call algorithm for taking user input.

Step II: Call algorithm for character repositioning schemes for modifying user-id/password.

Step III: Call algorithm for generating numeric intermediate OTP.

Step IV: Call algorithm for generating numeric final OTP

Distribution of Numeric OTP

Final OTP is divided into two parts and server sends these OTPs to user by email and message. Intermediate OTP is not been shared between server and user that have to generated from final OTP by using digit repositioning algorithm. Extraction of secret value for authentication is governed by the numeric value of intermediate OTP.

Extraction of Secret Value at User End and User Authentication

Step I: User fetch two parts of OTPs from email and message and combine them to generate final OTP. Intermediate OTP is generated from final OTP using digit repositioning algorithm.

Step II: Fetch the corresponding two characters from user id or password and security questions directed by the numeric value of first 4 digit of intermediate OTP. Fetch the bit value of pixel from biometric image governed by the numeric value from 5^{th} to last digit of intermediate OTP.

Step III: Converting the character values into binary and perform alternate merging among binary values of characters and pixel's block. Thus generate the secret octal value used for authentication. Server also executes Step II, Step III and generates secret value. Both the generated secret value at user and server end is being matched to validate the authentication.

RESULT AND DISCUSSIONS

Inputs at User Registration Time to Authentication System

User provides user id, password, unique biometric images and choice of character repositioning algorithm to server.

Server side OTP generation

Repositioning the characters of user-id by using character repositioning algorithm chosen by user

```
Enter user id: Harry123

Select any one Character Repositioning algorithm
for repositioning the characters of user id :-
1.Positional Reverse Odd Normal Even
2.Positional Reverse Even Normal Odd
3.Continuosly Reverse Odd Normal Even
4.Continuosly Reverse Even Normal Odd
Enter Your Choice        1

Modified user id is :- 2 a y r r 1 H 3
```

Repositioning the characters of user password by using character repositioning algorithm chosen by user

```
Enter the password: ab@#12CD

Select any one Character Repositioning algorithm
for repositioning the characters of password :-
1.Positional Reverse Odd Normal Even
2.Positional Reverse Even Normal Odd
3.Continuosly Reverse Odd Normal Even
4.Continuosly Reverse Even Normal Odd
Enter Your Choice        1

Modified password is :- b # 2 D a @ 1 C
```

Normal user-id and password will be used for authentication and modified user-id or password will be accessed for generating the values for user authentication.

Inputs of security questions and answers from user for OTP generation.

```
1.What is your first pet name      : Fluff
2.What is your first friend name   : Sejal
3.What is your favorite color      : Black
```

Inputs of user's biometric images for OTP generation.

```
Enter name of 1st Biometric Image:    BioImg1.jpg
Enter name of 2nd Biometric Image:    BioImg2.jpg
Enter name of 3rd Biometric Image:    BioImg3.jpg
```

The Images are:-



Biolog1.jpg Biolog2.jpg Biolog3.jpg

Randomize selection of positions of characters / pixels for intermediate OTP generation.

```
1. Random selection of User-ID/Password and
random selection of position of character from user-
id /password :                          2   8

2. Random selection of security question and
random selection of position of character from
answer :                                1   4

3. Random selection of biometric image, pixel and
block of pixel :                3   67110   2
```

Generation of Intermediate OTP

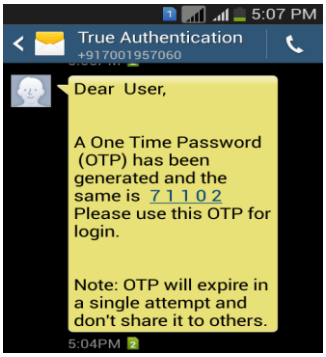
```
2 8 1 4 3 6 7 1 1 0 2
```

Generation of final OTP after repositioning the digits of Intermediate OTP

```
2 1 3 8 4 6 7 1 1 0 2
```

Distribution of OTP

Final OTP will be divided into two parts and distributed through email and SMS.



Formation of Final OTP at user end

```
Combining the OTP received in user email and SMS
2  1  3  8  4  6  7  1  1  0  2
```

Generation of Intermediate OTP after repositioning the digits of Final OTP at user end

```
2 8 1 4 3 6 7 1 1 0  2
```

Extraction of values from Intermediate OTP for authentication at server and user end

Extraction of values determined by Intermediate OTP

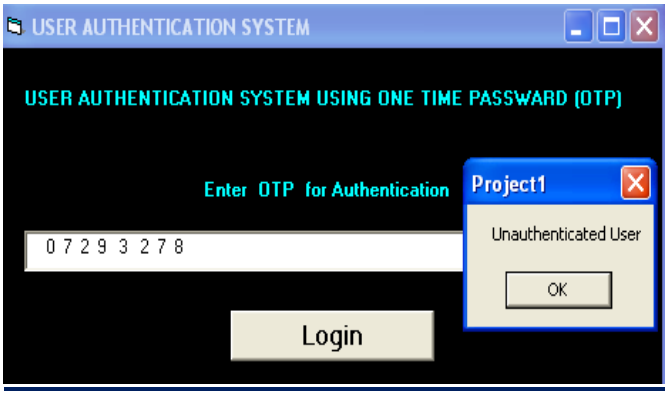
All the characters determined by the Intermediate OTP will be fetched from modified user-id or password not from normal user-id or password.

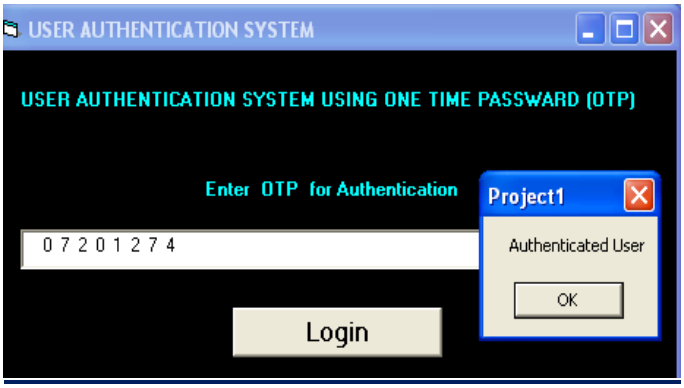
```
Fetching 8th character from user modified password
:  C
Fetching 4th character from 1st security question 's
answer :  f
Fetching bits of 2nd block of  67110  numbered
pixel from  3rd biometric image :  01001010
```

Conversion of fetched characters into bits and generation or secured values for authentication

```
Conversion of values into 8 bit binary representation:-

8 bit representation  of  ASCII value (67) of
character ' C ' is:                  01000011
8 bit representation  of ASCII value (102) of
character ' f ' is :                 01100110
8 bit value of 2nd block of  67110  numbered  pixel
from  3rd biometric  image is :      01001010

 Alternate merging of binary values and formation of
octal value corresponding to binary value
     000  111  010  000  001  010  111  100

Generation of secured  value for user authentication
          0  7  2  0  1  2  7  4
```

User authentication





Comparison between Existing OTP System and Security Analysis

Table- I shows the comparison between existing OTP based authentication system.

Table 1: Comparison with existing OTP based authentication system

Name of proposer	Core idea
Y. Huang, Z. Huang, H. Zhao,X. Lai [1]	OTP based on time stamps and sequence numbers.
N.Vishwakarma, K. Gangrade [2]	Random image and text based OTP with SHA-512 algorithm.
Ananthi Sheshasaayee , D. Sumathy [3]	OTP is encrypted and cipher text is encrypted by steganography and distributed. Personal Identification Number (PIN) needed to decrypt the OTP
WenBin Hsieh, Jenq-Shiou Leu[4]	Volatile OTP based on time and location of mobile device of user.
Proposed system	Randomize selection of bit values and pixel's block from user personal information and biometric image based OTP.

Table 2 shows security analysis of the system

Table 2: Security analysis of proposed system

Size of security defined parameters for OTP formation	**Number of executions needed to generate all possible combinations of the security parameters to originate OTPs**
For Intermidiate OTP Size of both user id and password are 8 chars. Number of security questions -3 Answer of all 1st , 2nd and 3rd questions has 5 characters . Number of biometric image-3 Size of all 1st, 2nd, 3rd images is 108*98 pixels (108*98*32 bits).	*For Intermidiate OTP* {Factorial(8)*[factorial(8) /(factorial (1) * factorial (8-1))]+1} * {[factorial(5) /(factorial (1) * factorial (5-1))]+1} * {[factorial(108*98*32) / (factorial (8) * factorial (108*98*32-8))]+1}
For Final OTP Size of intermidiate OTP is 11 characters.	*For Final OTP* Factorial(11)
For Extracting secured values for authentication Size of both user id and password are 8 chars. Number of security questions -3 Answer of all 1st , 2nd and 3rd questions has 5 characters . Number of biometric image-3 Size of all 1st, 2nd, 3rd images is 108*98 pixels (108*98*32 bits).	*For Extracting secured values for authentication* {Factorial(8)*[factorial(8) /(factorial (1) * factorial (8-1))]+1} * {[factorial(5) /(factorial (1) * factorial (5-1))]+1} * {[factorial(108*98*32) / (factorial (8) * factorial (108*98*32-8))]+1}

Total numbers of executions needed to generate all possible combinations of the security parameters to originate OTPs are

Factorial(11) + 2 * [{Factorial(8)*[factorial(8) /(factorial (1) * factorial (8-1))]+1} * {[factorial(5) /(factorial (1) * factorial (5-1))]+1}* {[factorial (108*98*32) / (factorial (8) * factorial (108*98*32-8))]+1}]. These amounts of executions will take extreme amount of time still the system can't be hacked as user private information and biometric images are secured from the unauthenticated user. So the system is extremely secured.

CONCLUSIONS

Six levels of securities are present in the proposed system. User id and password based authentication, random selection of characters or pixels from randomly selected security authentication text or biometric image objects, distribution of OTPs in multiple communication mode, formation of separate OTPs for distribution (final OTP) and user authentication (intermediate OTP), extraction of secured values from user private information for authentication defined by intermediate OTP and generation and use of derived secret value for authentication rather than using OTP values.

Random selection of characters and pixels from randomly chosen user private information provides more security as if the OTP is hacked still the secured authentication value can't b retrieved without user biometric unique image, user id, and password and security questions. Thus security is increased.

Formation of separate OTPs for distribution (final OTP) and user authentication (intermediate OTP) impose a great security as separate digit repositioning algorithm is needed to convert final OTP into intermediate OTP. So if the final OTP is being hacked at the time of distribution still the system is secured.

Distribution of OTPs into parts through different communicational channels (email and SMS) increase security level as multiple number of hacking is needed to access the entire OTP.

Proposed system extracts and uses secured values for authentication from user private information (biometric image, user id, password and security questions) defined by intermediate OTP. So if the OTPs are being hacked still the system is secured due to the unavailability of user private information. Thus enhance the security in great extant.

.

REFERENCES

[1] Yun Huang, Zheng Huang , Haoran Zhao, Xuejia Lai, "A new One-time Password Method" ScienceDirect, DOI: 10.1016/j.ieri.2013.11.006, [International Conference on Electronic Engineering and Computer Science, 2013] , IERI Procedia (4), pp 32-37,2013

[2] Neha Vishwakarma, Kopal Gangrade, "Secure Image Based One Time Password," "International Journal of Science and Research (IJSR)", vol. 5, issue. 11, pp 680-683, November ,2016.

[3] Ananthi Sheshasaayee, D. Sumathy, "A Framework to Enhance Security for OTP SMS in E-Banking Environment Using Cryptography and Text Steganography" Springer, Singapore, DOI: https://doi.org/10.1007/978-981-10-1678-3_68, [Proceedings of the International Conference on Data Engineering and Communication Technology,] , Advances in Intelligent Systems and Computing book series (AISC, volume 469), pp 709-717,2016.

[4] WenBin Hsieh, Jenq-Shiou Leu," Design of a time and location based One-Time Password authentication scheme", DBLP, DOI: 10.1109/IWCMC.2011.5982418, [Proceedings of the 7th International Wireless Communications and Mobile Computing Conference, IWCMC 2011,] Istanbul, Turkey, July, 2011.

[5] Safa Hamdare, Varsha Nagpurkar, Jayashri Mittal, "Securing SMS Based One Time Password Technique from Man in the Middle Attack," "International Journal of Engineering Trends and Technology (IJETT)", vol. 11, issue. 3, pp 154-158, May ,2014.

[6] Navpreet Kaur , Mandeep Devgan , Shashi Bhushan, " Robust login authentication using time-based OTP through secure tunnel" IEEE, [3rd International Conference on Computing for Sustainable Global Development] ,New Delhi, India, March,2016.

[7] Tamanna Saini, "One Time Password Generator System," "International Journal of Advanced Research in Computer Science and Software Engineering", vol. 4, issue. 3, pp 781-785, March ,2014.

[8] Digital content for OTP , link " https://en.wikipedia.org/wiki/One-time_password".

[9] Digital content for OTP procedure, link "https:// www.bobcards.com /otp-procedure.htm".