International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

One Time Password Generation based on Random Permutation using User Identity with Timestamp

Shakir M. H. Al-Farraji, Huda K. Saadeh

Abstract*: A password is a string of alphanumeric elements that is used mainly to authenticate user identity in order to give permission gaining access to the computer resources that should be secured from any unauthorized access. For this reason, password need to be kept secure among different types of attack. One way to increase the security of gaining access to any computer resources is the using of one-time password as a two-factor authentication which is generated for using it only one time. In this paper, we introduced a new method to generate a one-time password that depends on the user identity such as user account name or password and the timestamp. This information is gathered to make a string that will be used to generate a random permutation of a given size. The process of generating random permutation is a one-way hashing method. From the generated random permutation, the one-time password is constructed with a flexibility of having different size as needed.

Keywords*: Authentication, one-time password, one-way hashing, random permutation, security.

I. INTRODUCTION

Using internet applications either through PCs, Servers, Mobile devices or any other internet connected devices is massively increased in the few past years [1], [2]. Some of these applications are public and do not influence their users with regards to security breaches. Other types of applications provide services delivered to specific users, and therefore, require user's identities checking mechanisms [2]. Granting user to access any type of service needs to check his/her account name and password in order to protect unauthorized individuals from gaining access to the service. These checking mechanisms are usually known as authentication [3]. Authentication process is a key factor in maintaining system's and user's security by limiting systems and services access to legitimate authorized users, and preventing intruders from disclosing systems' information, user's privacy or performing various types of attacks [4].

Various authentication techniques have been developed in literature based on Asymmetric and Symmetric cryptography [5], [6], [7] along with certificates issued by trusted third party certificate authority [8], [9]. Certificates are used to sign information and code segments in order to authenticate these information owners or creators which in turn increases the trust of these information [8]. User's authentication is performed through three concepts: something users have such as ID Cards. Something users know such as passwords or secret keys. Something users are such as biometric measurements using fingerprints, iris, and face recognition [10].

Cryptographic authentication techniques are based on secret keys to authenticate users. Keys management including key stores and shared keys distribution is considered a challenge for authentication techniques developers [11]. Using the same key for multiple communications and connections rises the risks of key leakage by attackers. Without any doubts, using one key or password per each communication harden the task of attackers [2]. One Time Password (OTP) is a collection of printable characters that are randomly generated. Many applications can benefit from OTPs such as accessing VPNs, and login into Wi-Fi [12]. There are many methods for sending and exchanging OTP three of them is mentioned: First, email based where OTP is generated on the server side and send it as an email to the client [10]. Second, SMS based where OTP is generated on the server side and send it as a text message to the client phone [11], [10]. Third, Application based where OTP is generated on the user side by using a specific smartphone application that scans a QR code on the screen [13]. Unfortunately, One Time Password (OTP) has many challenges: First, password generation algorithm which is based on random and pseudo-random algorithms should be resistant to different types of attacks such as predicting attacks. Second, managing and memorizing this number of OTPs is not an easy task for users [4], [11]. A Non-Exchanged Password Scheme is proposed by [14] for Password-Based Authentication in Client-Server Systems.

Two-Factor authentication techniques are used to increase security by using double layer of security and many of these techniques are implemented using special devices and facilitated by using OTPs [4], [12]. Authentication of user account and his password is done by creating a double layer gateway before granting access to the service.

Revised Manuscript Received on April 27, 2020.
* Correspondence Author

Shakir M. H. Al_Farraji *, Computer Science Department, Faculty of Information Technology, University of Petra, Amman, Jordan. Email: shussain@uop.edu.jo

Huda K. Saadeh, Department of Information Security, Faculty of Information Technology, University of Petra, Amman, Jordan. Email: hsaadeh@uop.edu.jo

The first layer is responsible to validate the user account name and password. The second layer is to authenticate this validation by creating the one-time password which is generated randomly during each time the user need to use the service. Many patents have proposed two-factor authentication tokens such as [15] and [16] patents.

Earlier authentication techniques require extensive computing resources. For that reason, they are not considered for Internet of Things (IoT) resources-limited devices such as sensors and mobile phones [17]. There are many researches currently focus on light-weight authentication techniques that suit IoT systems [17]. This paper focuses on a new method for generating a powerful and secured OTP that can be used in any application needs authentication.

This paper presents a new method for generating a secured and powerful OTP that can be used in any online application that needs additional authentication. The rest of this paper is organized as follows: section II provides literature review on OTP generation methods and its usage. In Section III, the proposed method is given by presenting a new algorithm which uses the user identity and timestamp in order to apply them into the String Based Random Permutation [18]. Section IV demonstrates examples of different OTPs generation and summarizes results with discussion. Finally, a conclusion for this work is given in Section V.

II. LITERATURE REVIEW

OTPs research can be classified according to their techniques and according to the attacks they resist. Among the earliest techniques is cryptographic OTP such as lamport [19] where the cryptographic chain of OTPs hashes is computed to be used for successive authentication verification. HOTP has developed OTPs using HMAC [12]. The strength of this approach is that it is flexible to be implemented in software and in hardware such as USB dongles to increase interoperability. Adding timestamps into HMAC to protect against replay attacks has been proposed in [20], where time is considered as a moving factor that enables the generation of short-term unique OTPs. Authors of [21] have added sequence numbers with timestamps to generate unique OTPs, and the technique has been tested in a two-factor authentication prototype in mobile phones. Using AES algorithm to generate efficient OTP for user authentication is proposed in [5]. RSA is used in [6] to encrypt the generated OTP to be used later by the user in cloud authentication.

Using biometric information in authentication was promising for the fact that each person has a unique biometric information. Meanwhile, using this static information is vulnerable to attacks once they are leaked [22]. For this reason, using biometric features to generate OTPs can be found in literature to enhance authentication security. Authors of [2] have proposed an OTP generation technique using features obtained from user fingerprint to overcome braking randomness attacks. Another technique has been proposed in [23] where OTP is generated fully randomly on a server and sent back to users in order to be used in two-factor authentication with his biometrics, the whole system is designed to gain the benefit of quantum computing to generate quantum OTPS (QOTP). Authors of [22] have proposed their method for generation of a one-time transformation for biometric features and enrolled template of a user to be used in user authentication to protect these biometric templates from eavesdropping and replay attacks over insecure internet. A DNA-Based cryptographic key generation algorithm is proposed by [24] which can be used and adapt to generate the OTPs for authentication.

Securing clouds using OTPs has been studied by many researchers. In [25], a data protection mechanism has been proposed by storing encrypted version of information on cloud and users are required to use additional time-limited valet key token after using OTP authentication to control their access. The proposed work in [4] has focuses on designing a privacy-aware architecture in the cloud to outsource the second factor of the two-factor authentication OTP to handle the OTP provisioning problem occurred in similar OTP service provider.

Studying authentication techniques for IoT has been also considered in the literature. In [10] a locker security system using IoT is proposed. A face captured by a camera is identified by a recognition algorithm once a valid PIN is entered to the locker keypad, in case of matched features an OTP is sent to the locker owner via email and an SMS to be verified. Otherwise the unmatched face is logged into the system and the owner is informed to contact police. Authors of [26] have proposed a smart ration card system with RFID tags and a verifier connected to the AWS database to overcome the shortages found in the classical ration distribution system. OTPs are sent to users to accomplish the verification process through their mobile phones.

Other techniques have been proposed in [27], a set of OTPs has been generated to be used by a user to login into browser accounts with the cooperation of universal replay-resistant secure authentication server which decrypts and substitutes the OTPs into the real passwords.

III. PROPOSED METHOD

The proposed method for generating one-time password uses the user account name and/or his/password with the date and time of the system and concatenate this information to make a string. The constructed string will be used to generate random permutation of any given size such as 64 or 128 or any size up to 256. The String Based method (SBRP) [18] is used to generate random permutation, then collect set of values from the generated permutation according to the required length of OTP in order to produce the OTP.

The following is a full description of this proposed method:

1. Obtain the user account name or the password or both to make a first string called S1.
2. Obtain the date and time from the system that consist of eight elements as follows

MS	S	M	H	DN	MN	D	Y

Where
MS: millisecond
S: second
M: minute

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

H: hour
DN: day name (three characters)
MN: month name (three characters)
D: day of the month (two digits)
Y: year (four digits)

These elements are stored in the second string called S2

S2 = MS+S+H+M+DN+MN+D+Y

where the + sign means concatenation process

3. Concatenate S2+S1 to make the new string called S
4. Determine the required permutation size (say 128)
5. Determine the required OTP size (Osize); where the size is number of OTP elements
6. Apply the SBRP method to the string S and Osize to generate the random permutation (P)
7. Construct the OTP as follows:

```
For i=1 to Osize
    j = P[P[i]]%126
    If j >32
        OTP[i] = char(j)
    else
        OTP[i] = j
```

In step 7, each OTP element is chosen arbitrary by taking the permutation position (index) defined by P[i], so P[i] is the index of the OTP element in P.

IV. ILLUSTRATED EXAMPLES AND RESULTS

To show the generation of OTP, let us determine the needed information that will be used to produce OTP. Let us consider the following:

User account name: shakir
S1 = shakir
Permutation size: 128
OTP size: 8

Date and time elements as explained in the proposed method:
S2=50:53:22:09:Sun:Feb:23:2020
Now construct S = S1 + S2 as a concatenation
S = shakir50:53:22:09:Sun:Feb:23:2020

Apply SBRP method on S to generate random permutation P of size 128 as follows

P:
80 48 109 0 54 76 10 8 114 106 96 70 88 17 32 108 92 112 21 62 23 12 41 27 33 24 95 29 39 4 83 42 45 47 16 94 6 28 50 58 61 65 68 111 71 77 116 82 86 98 107 59 118 73 104 5 123 126 127 125 122 117 101 120 103 11 99 87 38 85 79 74 121 105 75 69 55 67 18 102 66 89 63 100 60 13 81 91 51 49 46 44 43 115 72 36 40 110 37 30 113 97 93 25 57 22 1 2 3 14 26 56 124 7 19 53 15 90 9 34 119 84 52 31 78 64 35 20

Now, we will take the first eight values of the generated permutation; where these values represent the index of OTP values in this permutation.

Table I, shows the steps of constructing the OTP elements from the generated permutation by using the SBRP method. Modula 126 is applied for the obtained values and then each value greater than or equal to 33 is converted into its equivalent character in order to obtain the printable OTP elements.

Table I: Generation steps of OTP from the generated permutation(P)

Indices of the first 8 element of P	80	48	109	0	54	76	10	8
Values of indices %126	66	86	14	80	104	55	96	114
Value>=33 take char	B	V	14	P	h	7	`	r
OTP elements	**B V 14 P h 7 ` r**							

The same data given above concerning the user account name, permutation size, and OTP size are used in 10 different times generate different OTPs as shown in table II.

Table II: Generation different OTPs in different times with the same given username and permutation size and OTP size

Seq	OTP using user name =”shakir”, Perm size=128, OTP size = 8
1	R ^ % k + 4 E x
2	M 11 T 5 B 0 7 ^
3	12 J 24 10 x 4 5 22
4	S 4 2 < # o U |
5	l 1 B t 3 $ = 4
6	% 27 29 18 1 4 1 l
7	A p o & r [s 23
8	e 30 32 P 0 23 9 10
9	G K 6 f N v {]
10	[% i * = ; V ?

In Table III, different usernames are used with the same permutation size and the same OTP size generating different OTPs.

To show the power of this proposed method, another two examples are shown in table IV and table V. In table IV, the same user identity is given, and the same timestamp is given in different millisecond by constructing OTP every millisecond.

In table V, the same user identity is given and the same timestamp for 10 consecutive days in which all elements of the timestamp are fixed except the day of the week and the day of the month.

Table III: Generation different OTPs with different username only

Username	Perm size	OTP size	OTP
shakir	200	8	16 # : Z ? 18 23 3
computer	200	8	e , 3 19 W 3 24 &
OTP	200	8	F 19 26 O 26 1 18 29
john	200	8	18 } 9 “ 3 k r &
security	200	8	16 ? 1 11 3 a 22 19
sam	200	8	2 # . - I 29 14 #
sami	200	8	28 g 22 12 61 0 H h
fisher	200	8	E K G 10 H * p C

Table IV: Generation different OTPs with different millisecond of timestamp

user identity=”john” Perm size=200 OTP size=8	
Timestamp	**OTP**
10321009SunFeb022020	H - > 2 l 1 21 /
11321009SunFeb022020	“ 13 1 Q 2 ` } 5
12321009SunFeb022020	L 18 29 32 > 8 R Y
13321009SunFeb022020	N 30 32 Z 0 > 6 I
14321009SunFeb022020	P 3 + 18 @ 32 22 8
15321009SunFeb022020	+ ‘ 23 - y z } C
16321009SunFeb022020	T } 25 11 E ; 23 32
17321009SunFeb022020	21 32 ? B P ! U 2
18321009SunFeb022020	X 15 3 & 32 ^ : 12
19321009SunFeb022020	18 18 3 16 “ 13 G &

Table V: Generation different OTPs with different day of timestamp

user identity=”john” Perm size=200 OTP size=8	
Timestamp	**OTP**
80321009MonFeb102020	29 % 21 f 2 20 : q
80321009TueFeb112020	g % ! a 2 20 T 10
80321009WedFeb122020	‘ % w \ 2 20 12 q
80321009ThrFeb132020	$ % # e 2 20 14 10
80321009FriFeb142020	a % z O 2 , T q
80321009SatFeb152020	# % } V 2 20 > q
80321009SunFeb162020	# % h 8 2 20 x q
80321009MonFeb172020	m % 8 f 2 20 14 q
80321009TueFeb182020	t % 17 w 2 20 8 7
80321009WedFeb192020	& % v \ 2 20 l q

A. Results and discussion

The result of this proposed method for generating a one-time password shows its power through the different OTPs that are generated which are presented in Table II and Table III. Same user account name or password or email address is used with the same permutation size and same OTP size and these data are compound with date and time (timestamp) which is taken from the system shows that different OTPs are generated each time this proposed method is used. Also, different OTPs are generated even when the input is the same user identity and the same timestamp in different millisecond as shown in table IV which 10 different OTPs are generated with the same user identity and timestamp in 10 consecutive milliseconds which is suitable for multiuser online applications.

Table V shows different OTPs are generated for 10 consecutive days of the same month and all other timestamp elements are the same. The generated OTP is a product that comprise the user entity such as name, account name, email, password and the system date and time in addition to another information that is set by the method to determine the permutation size. This mixture of information is used to generate random permutation by using the SBRP method to get advantages of this powerful patent method in order to produce different OTPs.

V. CONCLUSION

One-time password is playing main role for two-factor authentication system to strengthen the security of internet-based/online application. The new method for generating one-time password is described in this paper which includes the algorithm and an example illustrating all steps to construct one-time password. The power of this proposed method came from compound user identity and timestamp and the one-way hashing function that generate random permutation which is used to construct the one-time password. Two-factor authentication schema has used the OTP approach with a different authentication scenario, the proposed OTP generation method in this paper can be easily implemented for any authentication system of any online application.

REFERENCES

1. R. Dubey and J. S. Nair, "A Review on Secured One Time Password Based Authentication and Validation System," International Journal of Computer Sciences and Engineering, vol. 5, no. 6, pp. 232-236, 2017.
2. B. Cha, K. Kim and H. Na, "Random password generation of OTP system using changed location and angle of fingerprint features," in 8th IEEE International Conference on Computer and Information Technology, Sydney, NSW, Australia, 2008.
3. ArunKumar.Kasa and S. Ashritha.K, "A Survey Paper On User Authentication," IJREAT International Journal of Research in Engineering & Advanced Technology, vol. 1, no. 4, pp. 1-3, 2013.
4. E. Erdem and M. T. Sandıkkaya, "OTPaaS—One Time Password as a Service," IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 743 - 756, 2019.
5. E. P. Nugroho, R. R. J. Putra and I. M. Ramadhan, "SMS Authentication Code Generated by Advance Encryption Standard (AES) 256 bits Modification Algorithm and One Time Password (OTP) to Activate New Applicant Account," in 2nd International Conference on Science in Information Technology (ICSITech), Balikpapan, Indonesia, 2016.
6. Karthik, Chinnasamy and Deepalakshmi, "Hybrid cryptographic technique using OTP:RSA," in IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), Srivilliputhur, India, 2017.
7. P. V. Mankar, "Key updating for leakage resiliency with application to Shannon security OTP and AES modes of operation," in International Conference on IoT and Application (ICIOT), Nagapattinam, India, 2017.
8. N. Yosaka, I. Nishimura and T. Nagase, "Authentication and Certificate Managements of Unauthorized Intrusion in Ad-Hoc Networks, Problems and Solutions," in International Conference on Network-Based Information Systems, Tirana, Albania, 2011.
9. Y.-K. Lee, D. G. Lee, J.-W. Han and T.-H. Kim, "Home Network Device Authentication: Device Authentication Framework and Device Certificate Profile," The Computer Journal, vol. 52, no. 8, pp. 871 - 877, 2009.
10. N. Anusha, A. D. Sai and B. Srikar, "Locker security system using facial recognition and One Time Password (OTP)," in International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2017.
11. S. Ma, R. Feng, J. Li, Y. Liu, S. Nepal, Diethelm, E. Bertino, R. H. Deng, Z. Ma and S. Jha, "An Empirical Study of SMS One-TimePassword Authentication in Android Apps," in ACSAC '19: Proceedings of the 35th Annual Computer Security Applications Conference, San Juan Puerto Rico, 2019.

12. D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache and O. Ranen, "HMAC: Keyed Hashing for Message Authentication," RFC 2014, February 1997.
13. J. Murkute, H. Nagpure, H. Kute, N. Mohadikar and C. Devade, "Online Banking Authentication System Using QR-code and Mobile OTP," International Journal of Engineering Research and Applications (IJERA), vol. 3, no. 2, pp. 1810-1815, 2013.
14. Shakir M. Hussain and Hussein Al-Bahadili, “A Non-Exchanged Password Scheme for Password-Based Authentication in Client-Server Systems”, American Journal of Applied Sciences, NY, USA, 5(12): 1630-1634, 2008 ISSN 1546-9239.
15. K. Sawada, "Authentication System". Patent US8074075, Dec. 2011.
16. Z. Lu and H. Yu, "One time password generating method and apparatus". Patent US8184872, May 2012.
17. K. S. Roy and H. K. Kalita, "A Survey on Authentication Schemes in IoT," in International Conference on Information Technology, Bhubaneswar, India, 2017.
18. Shakir M. Hussain Al-Farraji, "Method and System Generating String Base Random Permutation". *USA Patent* 10.496.377, 3 12 2019
19. L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol. 24, no. 11, pp. 770-772, 1981.
20. D. M’Raihi, S. Machani, M. Pei and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm," RFC 6238, 2011.
21. Y. Huang, Z. Huang, H. Zhao and X. Lai, "A new One-time Password Method," IERI Procedia, vol. 4, no. 2013, pp. 32-37, 2013.
22. Y. Ueshige and K. Sakurai, "A proposal of one-time biometric authentication," in Proceedings of The 2006 International Conference on Security and Management, SAM'06, Las Vegas, NV, United States, 2006.
23. M. K. Sharma and M. J. Nene, "Two-factor authentication using biometric based quantum operations," Security and Privacy, pp. 1-21, 2020.
24. Shakir M. Hussain and Hussein Al-Bahadili, “A DNA-Based Cryptographic Key Generation Algorithm", the 2016 World Congress in Computer Science (worldcomp'16), the 2016 International Conference on Security and Management (SAM'16), Las Vegas, USA, 25-28/07/2016.
25. T.-Y. Lin and C.-S. Fuh, "Considerations of Emerging Cloud Computing in Financial Industry and One-Time Password with Valet Key Solution," in IEEE International Conference on Computer and Information Technology (CIT), Nadi, Fiji, 2016.
26. S. Shukla, A. Patil and B. Selvin, "A Step Towards Smart Ration Card System Using RFID & IoT," in International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 2018.
27. D. Florencio and C. Herley, "One-Time Password Access to any Server without Changing the Server," in International Conference on Information Security, Taipei, Taiwan, 2008.

AUTHORS PROFILE

Shakir M. Al-Farraji, (shussain@uop.edu.jo) He received his B.A. degree in statistics from University of Al-Mustansiriyah, Iraq, in 1976 and M.Sc. degree in Computing and Information Science from Oklahoma State University, USA, in 1984. In 1997 he received his Ph.D. degree in Computer Science from University of Technology, Iraq. From 1997 to 2008 he was a faculty member at Applied Science University, Jordan. Currently, he is an associate professor at Petra University, department of computer science, Faculty of Information Technology, Jordan. His research interest covers encryption, key generation, authentication, and data compression. He received a USPTO patent for generating random permutation and currently working on DNA based cryptography in encryption, authentication, and digital signature. He is a member of ACM.

Huda K. Saadeh, (hsaadeh@uop.edu.jo) She received her B.A. degree in Computer Science from University of Jordan, Jordan, in 2000 and M.Sc. degree in Image Processing from University of Jordan, Jordan, in 2006. In 2018 she received her Ph.D. degree in Information and Network Security from University of Jordan, Jordan. From 2001 to 2018 she was a faculty member at University of Petra, Information Technology Faculty, Computer Science Department. Currently she is an assistant professor at University of Petra, department of Information Security, Faculty of Information Technology, Jordan. Her research interest covers encryption, intrusion detection, IoT, and Network Security, Networking Architectures.