Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 8, August 2018, pg.37 – 52

COMPARATIVE STUDY ON ONE TIME PASSWORD ALGORITHMS

Dr. K. Mohan Kumar[1], G. BalaMurugan[2]

Research Guide & HOD of Computer Science [1], Research Scholar [2]
PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur 613 005, Tamil Nadu - India

ABSTRACT: Web applications play a major part in our day to day life. Every human being use computers for their transactions using web applications. Even personal information's are stored in government websites. Banks are using web applications for the transactions. Due to lack of security lot of frauds are occurred every day. So, security issue is an important issue in our digital life. One time pass word is the solution for this issue. Many algorithms are used to generate OTP. Every algorithm has its own pros and cons. This study analyse seven algorithms and suggest the best OTP generation algorithm using various aspects.

INDRODUCTION

One-Time Passwords (OTP) can provide complete protection of the login-time authentication mechanism against replay attacks. A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will

be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work. So we need to generate OTP. OTP generation algorithms typically make use of pseudo randomness or randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details [1].

Approaches for generation of OTP[1]

The various approaches for the generation of OTPs are listed below.

- Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)
- Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).
- Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter. The following Figure-1 shows how OTP is generated and used for the transactions.

Figure-1: Genation of OTP and usage

One- time password or PIN [2]

Static OTP is a password that is valid for only one login session or transaction, on a computer system or other digital device. A one-time PIN code is a code that is valid for only one login session or transaction using a mobile phone. It is often used in two factor authentication or 2FA to provide an extra layer of security for the user when he uses an ATM machine or tries to login to a service from a different computer. Since the one-time pin is valid for only a single use, they are not vulnerable as static passwords (passwords that do not change) and cannot be reused a second time by anyone, including unauthorized persons and

thus avoiding the threat of pin code the left. The following Figure-2 shows the screen shot of OTP login system.

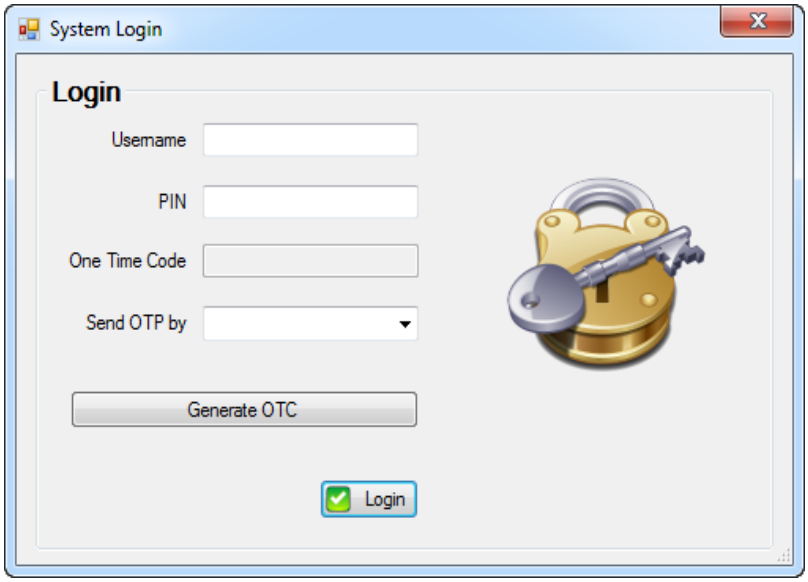

Figure-2: OTP login screen

There are number of ways to deliver one-time passwords and pins with the two most common and secure ways being through proprietary tokens and mobile phones. Using mobile phones for delivering OTP's come as a logical step due to mobile phones being ubiquitous and that most of them meet hardware requirements needed to successfully deal with OTP's. The usage of modern smart phones in delivering one-time PIN codes benefits both the end-users who are already familiar with their device and don't need to use another one and enterprises that need to deliver them, as using this method lowers their operational costs.

- Static password
- Replay attack.

Static Password

The impact of the Internet over the last few years has meant fundamental changes in the way the user access business systems. The network security perimeter has crumbled at all levels while the number of users waiting for the network access has grown. The geographical location of users has also widened to a situation where they can be, not just in a different department or company branch office, but anywhere in the world. While there are enormous productivity benefits available from increased access, the security risks have greatly

increased. The traditional method of securing system access was by authentication through the use of password [2]

Replay Attack

Replay attacks can be prevented by tagging each encrypted component with a session ID and a component number. Using this combination of solutions does not use anything that is interdependent on one another. Because there is no interdependency there are fewer vulnerability. This works because a unique, random session id is created for each run of the program thus a previous run becomes more difficult to replicate. In this case an attacker would be unable to perform the replay password [3]

Problem in OTP generation

Use of one time passwords (sOTPs) as a second step to logging in seems to be getting more popular recently. There are two main approaches to OTPs, the first being delivery of the OTP over a channel like SMS, and the other being a code that changes every time you use one to log in or on a predefined time schedule, based on a predefined algorithm. To use the first type, one must have a device with network connectivity and a phone number to receive SMS. With devices like RSA Secure ID tokens or Google Authenticator, a person can generate the second type of OTP manually generate the OTP on your mobile handset instead of receiving it through SMS. OTP application is available to Apple, Android, Windows and blackberry mobile users. OTP can be generated through an application without internet connection/Mobile network. Activation of this application will involve two steps as under: Downloading of Mobile OTP application "CA MOBILE OTP" on handsets. Users are required to download the application from respective app stores [4].

METHODOLOGY

Characteristics of OTP Methodology [4]

Encryption method is a binary additive stream cipher, where a stream of truly random keys is generated and then combined with the plain text for encryption or with the cipher text for decryption by an "exclusive OR" (XOR) addition. It is possible to prove that a stream cipher encryption scheme is unbreakable if the following preconditions.

- The message is represented as a binary string (a sequence of 0's and 1's using a Code mechanism such as ASCII coding).
- Ensure that the Key generated for the purpose of Encryption / Decryption is unique and that there will be no re-use of the same.
- Ensure that the selected/assignment of Key is completely a random function.
- Ensure that the total length of plaintext should be made equal to that of the generated key.

The following Table-1 shows XOR operation. Column A shows that a bit of plain text, column B as its corresponding key bit and column A^B is the resultant of XOR table.

A	B	A^B
0	0	0
0	1	1
1	0	1
1	1	0

Table -1 XOR operation

OTP encryption process

One Time Pad keys are used in pairs. One copy of the key is kept by each user and the keys are distributed securely prior to encryption. The confidentiality and authenticity of the One Time Pad keys are assured by continuous protection during their distribution and storage. This guarantees that outsiders will not be able to misuse the key (e.g. by copying or altering the key during distribution).

Currently, all the keys are exclusively generated by a "True Random Noise Source" and the noise source is integrated in the security system, which ensures tamper resistant protection. The following figure-3 shows in how to used encryption of OTP.

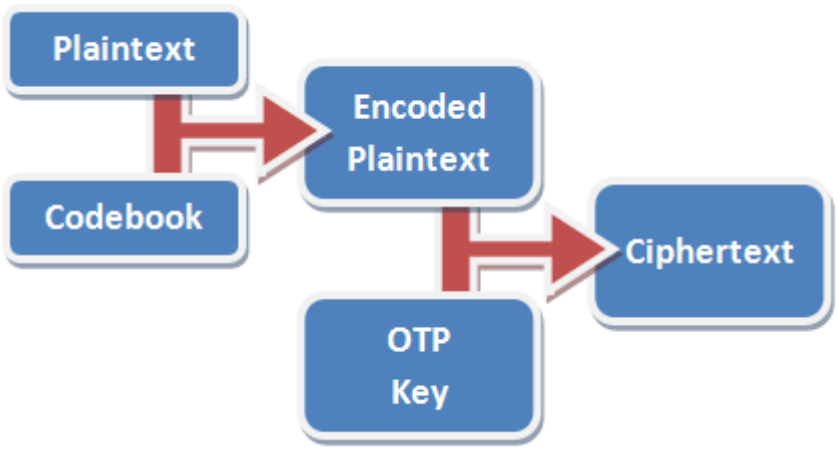

Figure -3 Encryption of OTP

Methods of OTP generation

Time-synchronized

A time-synchronized OTP is usually related to a piece of hardware called a security token (e.g., each user is given a personal token that generates a one-time password). Inside the token is an accurate clock that has been synchronized with the clock on the proprietary authentication server. On these OTP systems, time is an important part of the password algorithm, since the generation of new passwords is based on the current time rather than, or in addition to, the previous password or a secret key.

Mathematical algorithms

Each new OTP may be created from the past OTPs used. An example of this type of algorithm, credited to Leslie Lamport, uses a one-way function (call it f). The one-time password system works by starting with an initial seed s, then generating passwords f(s), f(f(s)), f(f(f(s))), ... as many times as necessary. Each password is then dispensed in reverse, with f(f(...f(s))...) first, to f(s). If an indefinite series of passwords is wanted, a new seed value can be chosen after the set for s is exhausted.

Various algorithms

1. Time based one time password algorithm [5]

This document describes an extension of the One-Time Password (OTP) algorithm, namely the HMAC-based One-Time Password (HOTP) algorithm, as defined in RFC 4226, to support the time-based moving factor. The HOTP algorithm specifies an event-based OTP algorithm, where the moving factor is an event counter. The present work bases the moving factor on a time value. A time-based variant of the OTP algorithm provides short-lived OTP values, which are desirable for enhanced security. The proposed algorithm can be used across a wide range of network applications, from remote Virtual Private Network (VPN) access and Wi-Fi network logon to transaction-oriented Web applications. The authors believe that a common and shared algorithm will facilitate adoption of two-factor authentication on the Internet by enabling interoperability across commercial and open-source implementations.

2. Hotp: hmac-based one-time password algorithm [6]

Home networks are one of the focused areas of research these days. One of the important services that home networks provide is to remotely control home appliances in home network. However, the remote control service causes home networks to have various security threats. Hence, home networks should provide strong security services, especially remote user authentication. Here provide an efficient solution for authentication scheme to provide secure remote access in home network environments. Our proposed scheme uses HMAC-based one-time password algorithm for the user authentication in home networks. The proposed scheme is not only has several advantage features but also quite satisfactory in terms of the security

Requirements of home networks. HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))

3. Lamport one time password authentication [7]

End-to-end authentication between devices and applications in Internet of Things (IoT) is a challenging task. In today's world of distributed data sources and Web services, remote client authentication is very important to protect customer's sensitive data over Internet. Common example of remote client authentication is the service like Internet banking. Existing authentication mechanisms are vulnerable to security crimes and threats

and can interrupt the progress of communication between the devices or application due to the complexity and heterogenity in terms of devices, topology, communication and different security protocols used in IoT. Therefore, Our proposed scheme uses the principles of lightweight Identity Based Elliptic Curve Cryptography scheme and Lamport's OTP algorithm. So, our scheme with a smaller key size and lesser infrastructure is the right candidate to perform the authentication without compromising the security level. Also this scheme can be implemented in real time IoT networks.

4. S/key one time password system [8]

The S/KEY system has several advantages compared with other one-time or multi-use authentication systems. The user's secret password never crosses the network during login or when executing other commands requiring authentication such as the UNIX passwd (change password) or su (change privilege) commands. No secret information is stored anywhere, including on the host being protected, and the underlying algorithm may be made public. The remote end (client) of this system can run on any locally available computer and the host end (server) can be integrated into any application requiring authentication. The S/KEY authentication system has been in experimental use at Bell core for two years. It is available by anonymous ftp on the Internet**.**

5. Two factor authentication in one time password [9]

Two-factor authentication (2FA) provides improved protection, since users are prompted to provide something they know and something they have. This method delivers a higher level of authentication assurance, which is essential for online banking security. Many banking systems have satisfied the 2FA requirements by sending a One Time Password (OTP), something possessed, through an SMS to the user's phone device. Unfortunately, international roaming and SMS costs and delays put restrictions on this system reliability. This paper presents a novel two-factor authentication scheme whereby a user's device produces multiples OTPs from an initial seed using the proposed production scheme. The initial seed is produced by the communications partners' unique parameters. Applying the many from one function to a certain seed removes the requirement of sending SMS-based OTPs to users, and reduces the restrictions caused by the SMS system.

6. Online banking authentication in mobile otp [10]

In online banking, security is an important issue for online banking application which can be implemented by various internet technologies and gap between real world and virtual world can be filled up. While implementing online banking system, secure data transfer need can be fulfilled by using https data transfer and database encryption techniques for secure storage of sensitive information. To eliminate threat of phishing and to confirm user identity, QR-code which would be scanned by user mobile device can be used and weakness of traditional password based system can be improved by one time password (OTP) which can be calculated by user transaction information and data unique at user side like imei number of the user mobile device.

7. Backup key generation in one time password [11]

The use of one-time password (OTP) has ushered new life into the existing authentication protocols used by the software industry. It introduced a second layer of security to the traditional username-password authentication, thus coining the term, two-factor authentication. One of the drawbacks of this protocol is the unreliability of the hardware token at the time of authentication. This paper proposes a simple backup key model that can be associated with the real world applications' user database, which would allow a user to circumvent the second authentication stage, in the event of unavailability of the hardware system.

The backup key is a 16 digit alphanumeric code with both uppercase and lowercase symbols. Each entry in the user database, i.e. every username-password pair, is associated with a unique backup key. That key would not be associated with any other pair within the user database. At the time of a user's registration, the backup key would be supplied to him and associated with his account. It is assumed that the user has kept it safe. In the event when he is barred at the second authentication stage (due to unavailability of the hardware token), he could enter this backup key and regain access to his account. Immediately, a new backup key would be generated and associated with backup key.

RESULT AND DISCUSSION:

The following Table-2 is created after analyzing the seven OTP Generation Algorithms. This table gives an overview of seven algorithms.

S. NO	Name of the algorithm	Implementation language	Benefits of algorithm	Drawback in algorithm
1.	Time based one time password algorithm	Java/Java x	➢ Human side security ➢ can be used in mobile phone applications ➢ OTP is 8 digit long numeric values ➢ OTP is valid for 30 seconds. ➢ OTP is generated Randomly	➢ Some time Failure in Receiving ➢ High Cost ➢ Easy to find the Secret key
2.	HMAC-based one time password in(Htop)	Open source/ Java x/Java f x script	➢ Ability to face the brute force attack with probability of success. ➢ ensuring frequent use in human time.	➢ some time Validation error will come ➢ Potentially valid for long time
3.	Lamppost's one time Password algorithm	Open source Core java Data structure/java	➢ OTP is generated within 60 seconds. ➢ Calculation is performed in 1000 iteration. ➢ Remote system issues is in challenge	➢ SMS Lateness ➢ Cost is high ➢ Incoming message might be blocked. .

			➢ User responds in one time password is easy. ➢ Using relativity unique identifier for OTP generation	
4	S/key one time password algorithm		➢ It can be easily and quickly added to any kind of operating system. ➢ We can connect it into SSL. ➢ username and password are more secure ➢ Transmitted over the internet. ➢ Terminal users are happy to use because of its easiness ➢ Ease of Learning ➢ Ease of Installation	➢ Time is reduced at some extent
5.	Two factor authentication in one time password	Java x /data structure	➢ International Roaming facility ➢ 2fauthentication OTP ➢ Support in VPNS WEP SSO,ADFS,LINUX MICROSOFT WIFI, applications	➢ Installation is very difficult ➢ Message Delays in plague delivery.

			➢ High security while sending OTP through SMS into user account. ➢ two-factor authentication in email service ➢ increased in flexibility and productivity of 2fauthentication	
6.	Online Banking Authentication System Using QR-code and Mobile OTP	Java x	➢ Suitable for Online net banking, authentication in house etc. ➢ OTP is generated Instantly in fund transfer ➢ Secured 2 factor authentication ➢ A very cost effective way of achieving a strong 2factor implementation of OTP ➢ OTP can be sent to the user's enrolled email account. ➢ Usage is very simple and Easy. ➢ View the transaction in online at any time.	➢ Sometime due to server error it takes very long time to get OTP. ➢ Very difficult in no network No battery on the phone and laptop. ➢ Lack of trust.

7.	Backup key generation in OTP security protocol	RDBMS/ Platform independent programming languages/My SQL	➢ Data base designed for real world applications. ➢ Back up is maintained for randomly generated alphanumeric OTP. ➢ Sophisticated for the increase in network attacks and signalled the need for better security. ➢ Backup key is a 16 digit alphanumeric code with both uppercase and lowercase symbols.	➢ Learning and understanding is difficult.

Table-2: Overview of OTP generation algorithms

The following Table-3 is generated by giving the values to the seven algorithms

ALGORITHM	ADVANTAGE	DISADVANTAGE	NET VALUES
Time based one time password algorithm	5	- 3	2
HMAC one time password algorithm	2	-2	0
Lamport's one time password	5	-3	2
S/key one time password algorithm	7	-1	6
Two factor authentication one time password algorithm	6	-1	5
Online banking authentication system and mobile phone OTP	6	-3	3
Backup key generation in OTP security protocol	4	-2	2

Table-3 Performance analysis

Here the S/key algorithm has a higher value compare with the remaining six algorithms. The HMAC algorithm has lower values. So the S/key algorithm is the best algorithm compare with the other algorithms.

The following figure-4 gives the graphical representation of the above table-3

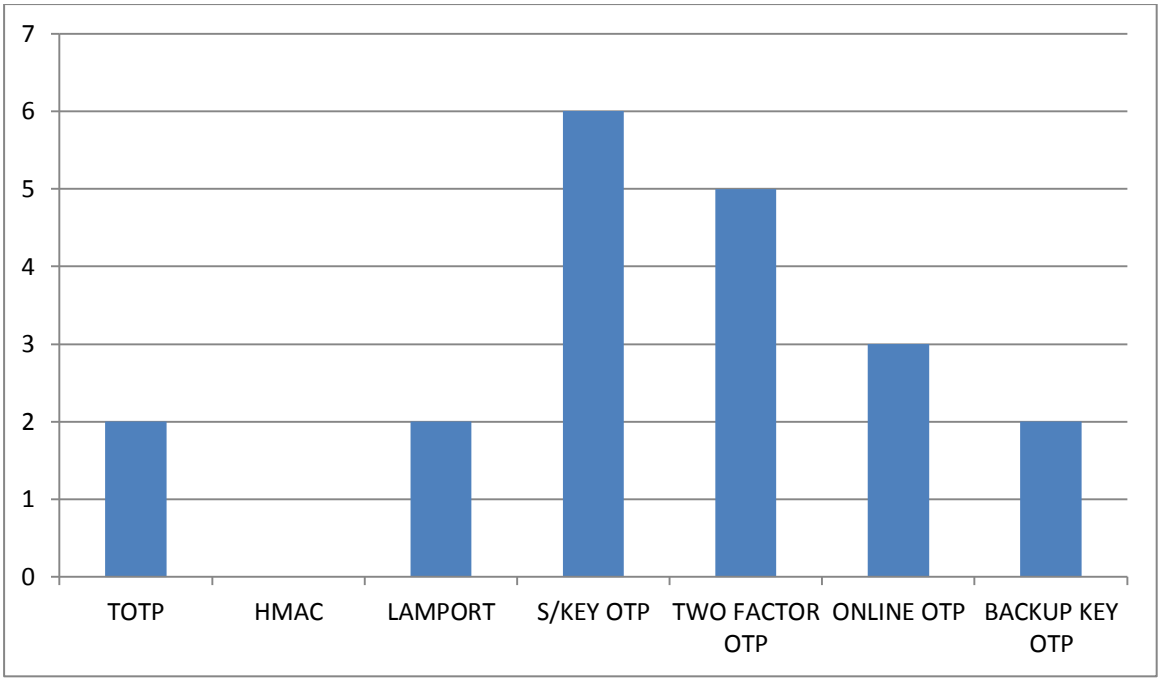

Figure-4 OTP performance analysis

In this study the s/key one time password algorithm is having more performance value 6. So this algorithm is an optimised algorithm used to generate One Time Password.

CONCLUSION

In OTP lot of algorithms are used to optimise the transactions. Each and every algorithm has its own advantages and disadvantages. In this study the various parameters of algorithms such as implementation language, merits and demerits are analysed and found that S/key one time password algorithm is an optimal algorithm which gives more performance value. So, the algorithm S/KEY gives better performance compare with other algorithms.

REFERENCES:

1. N. Haller, C. Mat z, P. Nesser, M. Straw, "A One-Time Password System", IEEE.
2. A.D.Ubin, "Independent One-Time Passwords", IEEE.
3. sarika khaladkar1, sarita malunjkar2 "Three –way security using image based authentication system" International Journal of Computer & Communication Technology ISSN (PRINT): 0975 -7449, Volume-6, Issue-2, 2017.
4. Neha Vishwakarma1, Kopal Gangrade2," Secure Image Based One Time Password" International Journal of Science and Research (IJSR).
5. Binod Vaidya1, Jong Hyuk Park2, hotp-based user authentication scheme in home networks" 978-1-4577-0737-7/11/$26.00 ©2011 IEEE.
6. Selman Yakut1 A. Bedri Özer1," hmac based one time password generator" 2014 IEEE 22nd Signal Processing and Communications Applications Conference (SIU 2014).

7. Thanushree.N.R1, Tejashree.N.R2," Integrating Lamport's One Time Password Authentication Scheme with Elliptic Curve Cryptography" International Journal of Recent Trends in Engineering & Research (IJRTER).
8. Neil M. Haller," The s/keytm one-time password system" 2014 28th International Conference on Advanced Information Networking and Applications Workshops.
9. Mohamed Hamdy Eldefrawy1," OTP-Based Two-Factor Authentication Using Mobile Phones" 2011 Eighth International Conference on Information Technology: New Generations.
10. Jaideep Murkute, Hemant Nagpure," Online Banking Authentication System Using QR-code and Mobile OTP" Sinhgad College of Engineering, Department of Information Technology, University of Pune, Pune-411041.
11. Jeyanthi N and Sourav Kundu," Backup key generation model for one-time password security protocol" IOP Conf. Series: Materials Science and Engineering 263 (2017) 042034.

