IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Survey on Enhancement of One Time Password as a Service (OTPaaS)

Siddharth S. Gosavi[1*], Gopal k Shyam[2],

[1,2] School of C & IT, School of Computer and Information Technology, Reva University, Bangalore, India

Corresponding Author: siddhugosavi89@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si14.193198 | Available online at: www.ijcseonline.org

Abstract— the traditional way of authenticating a user via Username and password is very much popular in digital world, where as for more security OTP is used, One Time Password is the technique which is two way authentications. This OTP technique can be used as service is cloud to users as One Time Password as service, in OTP as a cloud service some of the cloud service providers will provide this OTP for different cloud users for their online application login and website authentication. Cloud users can register their different web applications in the different cloud service. This will enable for this users access for accounts using OTP verification without maintaining many other passwords and several OTP accounts. In this paper author has given architecture for secure, privacy-friendly and trusted OTP provider and authentication phases are given. The purpose of doing survey of One Time Password as Service is to understand the need on one time password as service for authentication its fundamentals along with drawbacks of different authentication

Keywords— One Time Password (OTP), Authentication, Cloud, Two-factor Authentication, Multi-factor Authentication, cloud based OTP, cloud-based authentication service.

I.INTRODUCTION

Nowadays using internet is habits for some and need for some peoples and they use so many web applications, Services for which they do authentication with Traditional username and password method which needs to improve because unauthorized access is very much possible with today's technology. For this authentication user needs Username and password and they must have to memorize This credentials but again user does not use only one online Application so memorizing is quite a bit difficult task for Every application, along with this username is publicly Known to everyone so authentication is safe till user can Prove his/her identity with passwords which can be hacked By toweling or password guessing attack. There are many Author factors which prove password is not just safe way to Authentication as many issues are there like reusing similar Password for every online service. That is why, efficient Authentication Techniques are more preferable, especially when they are user friendly and it is believed that proposed System i.e. Cloud-based OTP architecture can help securing Authentication to many cloud services which user is using. OTP or One Time Password is well known for authenticating User with some random values, and also One Time Password Is Two factor authentication which is called as 2FA or TFA. TFA is very much Used cloud service. Authentication Of a user can be done with one of the three: knowledge, Possession, or inherence. Knowledge factor is the well known username and password Credentials. As this is widely used technique of authentication, almost in all Two Factor Authentication implementations include this factor. An inherence factor is related to user, is it a robot or what user is doing. Authentication can be done by biometric methods which can be either static (e.g., Fingerprint, Palm, and Retina scan) as well as dynamic (e.g., Hand waving, touch screen, keystroke, and voice). Authentication by this inherence helps for improving the problems of carrying tokens, remembering passwords, and for checking user identification. But, there are some problems come at the time of designing biometric authentication.

Four important issues can be as follows:

- Storage of delicate personal information is difficult
- Regeneration and reversal options must be available in case of password is stolen or else forgotten
- Biometric verification devices are costly and can't be always available, and
- Problem with Privacy occur when organizations Share the databases.

From this it is proved the Biometric authentication is difficult to adopt for day to day routine and for consistent users who uses services every time.

Possession factor is a commonly used authentication factor in TFA. In real time way to prove ownership is to agree on a value of pre-shared key. Due to which the structure of OTPs that can be generated based on the pre-shared key. This reason to produce many OTP's from the same single value is that management of a many pre shared keys is hard. OTP algorithms can be implemented as software or hardware where they named as software tokens or soft tokens, and inside hardware are known as hardware tokens or hard tokens. Nowadays mostly used smart-devices and smart-phones has changed the way of software keys and the ownership factor is now mostly used with the smart-phone with pre shared key(PSK) and OTP algorithm runs on the smart-phone as required for application of the service provider with respective users.

II. OUTLINE OF SURVEY

This survey is about an architecture that will give OTP solution for authentication to all online businesses. Current authentication Procedures needs credentials memorization and as well as they are not much safer from several attacks, along with the issue of bio-metrics is they are difficult to develop, maintain and they are costly .So it is necessity that the system will give safe and easy authentication using cloud based service i.e. OTP because OTP is a Two factor authentication and it is very effective way.

- **Objective**
  The reason of the survey of One Time Password as a service is to understand the need on one time password as service for authentication its fundamentals along with drawbacks of different authentication

- **Coverage and subject**
  The topics covered in this survey are authentication methods and OTP as service and its working along with what work can be done in it. Therefore the as per the subjects concern focus will be mainly on authentication procedures and cloud computing.

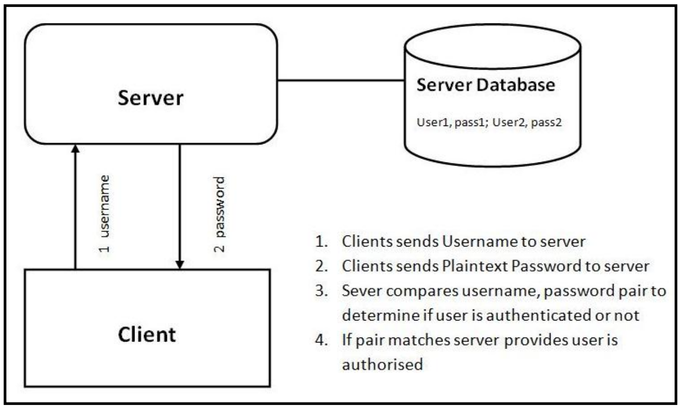
- **Date**
  This study and research for this survey is conducted from 15 October 2018 to 8 Jan 2019

III. BASIC CONCEPTS

1. Convectional Password based Authentication

The most straightforward, sadly still very normal, authentication strategy accessible is the conventional neighborhood authentication technique. In this system, username, password data as per authenticated client is pushed on the local server system. Clients will send their username's and password's in normal content to the server system, then this server system contrasts client's Authentication data and its nearby database.

In a event that gave username and password are found to coordinate, the client is viewed as confirmed. This is fundamentally the model utilized for user log in authentication on conventional multi client systems, and it has been copied various times inside different application bundles. Following is a diagram of the Convectional Authentication.



1. Clients sends Username to server
2. Clients sends Plaintext Password to server
3. Sever compares username, password pair to determine if user is authenticated or not
4. If pair matches server provides user is authorised

Figure 1.Convectional Password Based Authentication

There are many issues with this model which are as follows:

- Much of the time, client's passwords are put away in plain-content structure on the server machine. Any individual who can access the server's database approaches enough data to mimic any validated client.
- In cases in which clients' passwords are put away in scrambled structure on the server machine, plain content passwords are as yet sent over a conceivably unreliable system from the customer to the server. Anybody with access to the mediating system might almost certainly "snoop" [username, password] combines out of discussions and replay them to fashion validation to the system.
- Each different system must convey its own duplicate of every client's confirmation data. Thus, clients must keep up passwords on every framework to which they confirm, as are probably going to pick not exactly verify passwords for accommodation.
- Verification isn't reusable. That is, clients must validate independently to every framework or application they wish to get to. Thus, clients should more than once type their passwords and will in general pick less-than-secure passwords for accommodation.
- There is no endeavor made inside the model to cross-verify the server and customer. A framework which imitates the server framework can't be recognized by the customer from the real server, opening the likelihood of Trojan-horse servers gathering [username, password] sets and later utilizing them to confirm to the genuine server.

2. One Time Password

One time password (OTP) is a password that is legal for a single log-in session or exchange. OTP is broadly utilized as a password that isn't planted in the database, yet just as a solitary use password and quickly relinquished. The advantage of the OTP is situated on the distinctive application with a static password which is planted in the database. The utilization of scrambled static passwords is additionally not invulnerable from the assault by utilizing a key lumberjack or kind of it, in such a case that an aggressor figured out how to get the fundamental password and OTP password still login and exchanges won't be handled in light of the fact that the password is never again substantial. Code age as encryption is utilizing Message-Digest Algorithm 5 (MD5) which are broadly utilized with 128-piece hash esteem, this calculation has been generally utilized for security applications, password encryption, and uprightness trial of a record

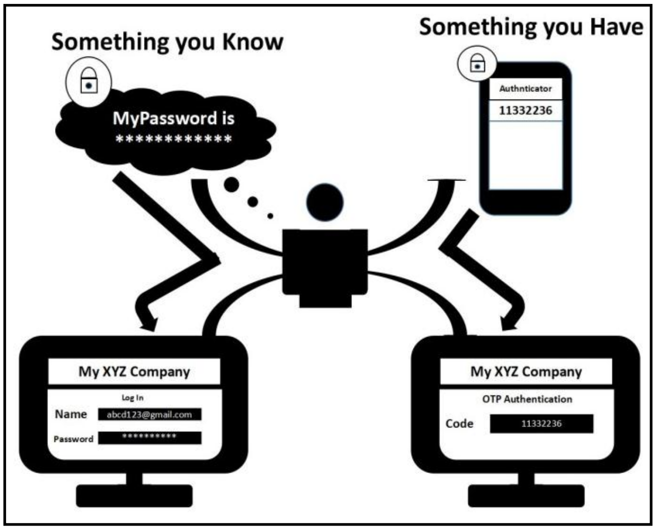


Figure 2.One Time Password

3. Multi Factor Authentication

In the process of Multi Factor Authentication, MFA will combine two or more independent credentials such as, client's password, client's security token and client's biometric verification. Objective of MFA is to generate a layered security mechanism so that it will become very tough to an unauthorized user to get access of location, computing device, network or database of the user. In case the one factor method is failed, then also it will become secure because attacker or hacker yet needs to cross one more security barrier to crack to successfully breaking into target.
The example for multi-factor authentication is Two Factor Authentication.

Two-factor authentication (2FA), Two Advance Check or Double Factor Authentication are some different names for TFA. TFA is another procedure for security check where the user needs to give two different credentials for authentication and to confirm their identity to ensure both the user's credentials and the assets the user can get. Two factor authentications has been shown more efficient security strategy which is better than other such as single-factor authentication (SFA).In SFA, user gives just a password. The Two factor authentication methods relay on users entering a password as well as a one more factor, which is generally a security key or else biometric factor which should be like a unique mark, facial scan etc.

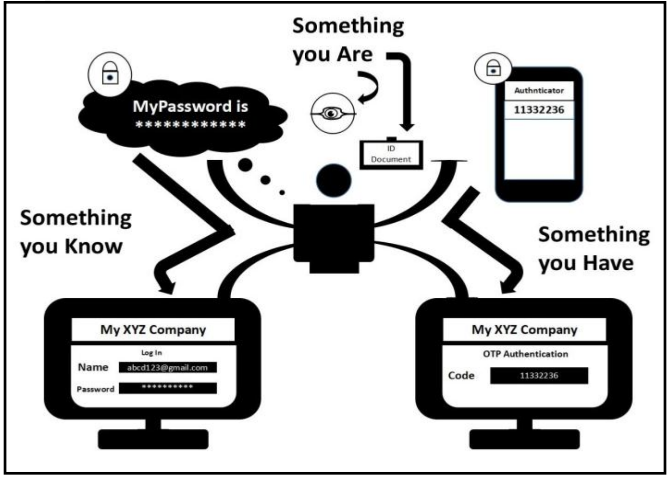


Figure 3.Two-Factor Authentication

The Multi Factor Authentication at very first stage performs Swiping a card and entering a PIN then Logging into a website and being requested to enter an additional one time password (OTP) that the website's authentication server sends to the client's phone or email address. After that Downloading a VPN client with a valid digital certificate and logging into the VPN before being granted access to network, Moreover swiping a card, scanning a fingerprint and answering security question. And in last Attaching a USB hardware token to a desktop that generates a OTP code and using the OTP to log into a VPN client.

4. Cloud Based OTP

The development in cloud shows that the Cloud Based OTP is more efficient than currently used Access control Technique. Cloud computing is an internet based service application. It provides various services which are IaaS, PaaS and SaaS. To access the cloud services, A cloud service provider will give a user log in details which are username and password. Whereas a log-in Details can be easily hacked or cracked as well as the security power of cloud computing low downs. From earlier days many authors used Two authentication mode in terms of mail conformation and one time password. In cloud computing an OTP enhances the security of access control.

IV. Review of the Relevant Literature

The Proposed system of Emir Erdem and Mehmet Tahir Sandkkaya [1] presents a diagram, essential security tips and also required conventions for cloud based One Time Password administrations to push little to medium ventures and people to move their ordinary username and password based verification plans to a progressively secure OTP-based TFA conspire. Security and protection issues of moving the

One Time Password administration to the cloud is taken cautiously. Conceivable defects and their belongings are talked about. It ought to be mentioned that the proposed design does not plan to explain the defects of customary username and password utilization, for example, retaining issue or defenselessness against speculating assaults. Conversely, adding a second factor to regular verification is the consequence of the aforementioned issues. This is a typical methodology since issues emerging from human instinct are difficult to forestall. A sensible use situation is recognized together with its assault demonstrate. The security criterion for a nonexclusive cloud-based OTP arrangement is characterized. At that point, a cloud-based OTP benefit engineering is structured.

The reasonable structure's security investigation demonstrates that the design and the conventions are hearty and sound. Conceivable focal points of the plan are tended to both from the viewpoint of an administration giving organization and an individual administration client. he engineering is a stage for reception of no master little to medium undertakings to more secure verification procedures than customary ones. The proposed methodology is viable as a two factor verification security instrument and gives numerous configurable choices by plan. Client profiles are available to future improvement at client gadgets, for example, standard password the board, certification the executives, etc. The plan gives organizations a chance to spend less on OTP-based TFA change both in the viewpoints of experience, businesses, equipment and programming. Furthermore, it lets the clients to oversee a large number of their records effectively at one place, yet by means of unlink able profiles. It is trusted that redistributing OTP benefit in the cloud may likewise ease many cloud specialist co-ops mass OTP appropriation, as they don't require making extra investment. Given the aforementioned points of interest, it is trusted that the proposed engineering is an underlying advance for acknowledgment of such services.

The paper [1] shows aim to give a privacy friendly cloud based real time architecture which will give secure OTPs for users. These OTPs dynamically get changed at each time they are used based on a provided algorithm with respective to a pre shared secret key (PSK).

PSK is the proof of ownership. A decided algorithm generates OTPs that are different from the output of a random oracle. Mostly algorithm is responsible for generation of distinguished OTPs and their seed values. Seed value could be any counter value or else the current time based value. Both the seed and the PSK are given together to the algorithm to generate the respective OTP.

One time passwords concept originated by L. Lamport [2] he has given the concept of user password authentication when authentication is secure then also an attacker can read the system's data, and attack the communication. For this problem author has proposed a technique which assumes that a secure one way encryption function and can be created with a microcomputer in the user's terminal.

Secure one way encryption function this proposed method of L. Lamport is commercialized as S/KEY Authentication system proposed by N.Hallers [3]. This paper proposed to the first standardization Of OTPs in 1998. One type of network attack on system on the Internet is listening stealthily on system's network connections with acquire login id's and passwords of real clients. The caught login id and password are, at a later time, utilized access the system. The S/KEY One Time Password system is intended to counter such attack, called as a replay attacks.

In 2005 in USA, A group of people who were members of Initiative for Open Authentication (OATH) suggested this algorithm which is an HOTP or HMAC Based [4] One Time Password Algorithm. The paper presents first the setting around a calculation that creates One Time Password esteems dependent on HMAC [BCK1] and is named the HMAC Based One Time Password (HOTP) calculation. HMAC based OTP was used with smart cards and USB devices.

The extension of the One Time Password (OTP) Algorithm is given by D. MRaihi, S. Machani, M. Pei, and J. Rydell in [5],It says that in particular the HOTP algorithm, as characterized in RFC 4226, to help the time based moving variable.

HOTP algorithm indicates an occasion based OTP algorithm, where the moving component is an occasion counter. The proposed work in this paper is on the moving factor on a time value. A time based variation of the OTP algorithm gives fleeting OTP values, which are desirable for improved security. The proposed calculation can be utilized over a wide scope of system applications, from remote VPN get to and Wi-Fi arrange log on to exchange situated Web applications.

Petrica and Groza [6] contemplated on an expansion of Lamport's work [2]. As indicated by their proposition, there is no restriction on the quantity of confirmations can be performed. They utilized capacities over cyclic gatherings of numbers rather than hash works in Lamport's paper. Thus, it is guaranteed that various and questionable number of validation can be performed without requiring another arrangement of OTPs. Be that as it may, the need of something beyond time to figure all passwords is the disadvantage of their proposed solution.

An expansion of Lamport's plan was proposed by Eldefrawy et al. [7]. Their point was to understand the vastness and the imposition issues of the Lamport's conspire. For that reason, they utilized two diverse hash capacities: one for seed refreshing and one for OTP generation. Despite the fact that their suggestion illuminates the aforementioned issues, their convention is a test reaction convention. So as to create OTPs, the client needs the server to introduce the convention with a test. This is something unfortunate for an OTP validation.

Gong et al. [8] proposed a novel OTP verification plot utilizing sub-passwords. The client and the server verify each other commonly dependent on challenge-reaction components. Sub-password choice also, restoration are satisfied by irregular stage capacities. Secluded arithmetical tasks and hashes are connected to sub-passwords to create generally free OTPs. In the enlistment stage, the server produces a few sub-passwords and sends them to the client.
The client stores the sub-passwords while the server stores them in a permuted request. In the verification stage, first the client challenges the server for sub-passwords count. At that point, the server applies a similar convention to validate the client. After each fruitful confirmation sub passwords are restored dependent on beforehand shared change capacities. This plan is a respective convention and it very well may be conveyed from cloud.

Yassin et al. [9] proposed a cloud based unknown OTP on spire which does not require additional gadgets. Their plan relies upon asymmetric scalar-product preserving encryption (ASPE) and RSA advanced mark. In their plan, OTP supplier and specialist organization are not isolated as in the design in Section III. At the end of the day, the client is as yet confirmed by specialist co-op.

Cheng [10] proposed an OTP token that is portable and cloud-based. How a MasterCard like of plastic card can be utilized as equipment token while creating OTP was talked about. In the plan, PSKs are put away in an intermediary server and OTP age is done through that server. On the off chance that this plan is utilized with the design that will be mentioned in this paper, plastic card equipment token should be utilized also.

One time passwords are reasonable for some regions as they give solid security and permit lightweight execution. For instance, Vaidya et al. [11] proposed an OTP plot for home systems. Their answer uses HOTP and non monotic cryptographic conventions. They guarantee that hash chain strategy with keen card innovation can give a vigorous and productive verification system as hash capacities are lightweight to be utilized in smartcards.

Another plan was proposed by Liao et al. [12]. They think about that utilizing PDAs is increasingly useful contrasted with its choices. They contended that how an OTP can be created dependent on QR-codes. Since a great many people have advanced mobile phones as of late, additional gadgets thought not are essential.

An outstanding equipment OTP maker is Yubico Company [13]. Their YubiKey agrees to numerous systems. All things considered, equipment executions have unfortunate properties. In the first place, conveying a different gadget could be unreasonable for a few. Appropriation and firmware updates of equipment gadgets are moderate and exorbitant. Besides, if a gadget does not have suitable UI for PIN passage to produce OTPs, it might be powerless when stolen. These variables have prompted consider that product execution is handier.

It is realized that Yubico does not give individuals a chance to do firmware updates to its items, thinking about security. Be that as it may, this gives a portion of its old gadgets a chance to open to recently developed assaults after some time frame. Ceaseless equipment cost is required for organizations. An answer that is good with cloud administrations is Google Authenticator [14]. Their methodology is to ease the executives of discrete OTPs for Internet Administrations dependent on OATH measures.

V. CONCLUSION AND FUTURE SCOPE

This survey presents an outline, basic security tips similarly as required traditions for cloud-based OTP organizations to push little to medium endeavors and individuals to move their standard username and password based approval plans to a dynamically secure OTP-based TFA plot. Security and insurance issues of migrating the OTP organization to the cloud is considered warily. Possible AWS and their assets are inspected. Rational courses of action and defends are communicated. A reasonable use circumstance is identified together with its strike illustrate. The security criteria for a customary cloud-based OTP course of action are denied. By then, a cloud-based OTP organization building is arranged. The hypothetical arrangement's security examination shows that the plan and the traditions are vivacious and sound. Possible focal points of the arrangement are kept an eye on both from the perspective of an organization giving association and an individual organization customer.

REFERENCES

[1] Ieee transactions on information forensics and security, vol. 14, no. 3, march 2019 otpaas one time password as a service emir erdem and mehmet tahir sandkkaya ,member, ieee

[2] L. Lamport, password authentication with insecure communication, common. Acm, vol. 24, no. 11, pp. 770772, nov. 1981.

[3] N. Haller, the s/key one-time password system, document 1760,internet engineering task force, fremont, ca, usa, 1995. [online].available: https://www.ietf.org/rfc/rfc1760.txt

[4] D. Mraihi, m. Bellare, f. Hoornaert, d. Naccache, and o. Ranen,hotp: an hmac-based one-time password algorithm, document4226, internet engineering task force, fremont, ca, usa,2005. [online]. Available: https://www.ietf.org/rfc/rfc4226.txt

[5] D. Mraihi, s. Machani, m. Pei, and j. Rydell, totp: time- basedone-time password algorithm, document 6238, internet engineering task force, fremont, ca, usa, 2011. [online]. Available: https://www.ietf.org/rfc/rfc6238.txt

[6] B. Groza and d. Petrica, one time passwords for uncertain numberof authentications, in proc. 15th int. Conf. Control syst. Computer sci. (cscs), 2005, pp. 669674.

[7] M. H. Eldefrawy, m. K. Khan, k. Alghathbar, t.-h. Kim, and h.elkamchouchi, mobile one-time passwords: two-factor authentication using mobile phones, secure commun. Netw., vol. 5, no. 5, pp.508516, 2012.

[8] L. Gong, j. Pan, b. Liu, and s. Zhao, a novel one-time password mutual authentication scheme on sharing renewed finite random sub passwords, j. Comput. Syst. Sci., vol. 79, no. 1, pp. 122130, 2013.

[9] 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 (lecture notesin electrical engineering), y.-h. Han, d.-s. Park, w. Jia, and s.-s,yeo, eds. Ordrecht, the netherlands: springer, 2013, pp. 423431.

[10] F. Cheng, security attack safe mobile and cloud-based onetimepassword tokens using rubbing encryption algorithm, mobilenetw. Appl., vol. 16, no. 3, pp. 304336, 2011.

[11] B. Vaidya, j. H. Park, s.-s. Yeo, and j. J. Rodrigues, robust one time password authentication scheme using smart card for home network environment, comput. Commun., vol. 34, no. 3, pp. 326336,2011.

[12] K.-c. Liao, w.-h. Lee, m.-h. Sung, and t.-c. Lin, a one-time password scheme with qr-code based on mobile phone, in proc.5th int. Joint conf. Inc. (ims idc), 2009, pp. 20692071.

[13] Yubikey. Accessed: mar. 20, 2017. [online]. Available: https://www.yubico.com

[14] Google authenticator. Accessed: mar. 20, 2017. [online]. Available: https://github.com/google/google-authenticator/wiki

Authors Profile

Mr. Siddharth Suresh Gosavi pursed Bachelor of Engineering from Pune University, Maharashtra in 2006 and perusing Master of Technology in Computer Science from Reva University.

Dr. Gopal Kirshna Shyam received BE and PhD in Computer science and engineering from VTU, Belagavi His research interest includes Cloud Computing, Grid computing, High performance computing etc.

He has published about 10 papers in highly reputed National/International Conferences like IEEE, Elsevier etc. and 5 papers in Journals with high impact factor like Elsevier Journal on Network and Computer Applications and International Journal of Cloud computing (INDERSCIENCE). His research articles on Cloud computing co-authored by Dr. Sunilkumar S. Manvi have been cited by several researchers. He is a lifetime member of CSI and is actively involved in motivating students/faculties to join CSI/IEEE/ACM societies.