

MULTIPLE SERVICE AUTHENTICATIONS WITH CLOUD OTP AS A SERVICE

S.Pradeep Kumar¹, R.Sundar², B.Anandraj³, B.Galeebathullah⁴

¹Professor, Department of CSE, Saveetha School of Engineering, SIMATS, Chennai. India.

^{2,3,4}Assistant Professor, Department of CSE, Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India.

Email: spradeepkumar272@gmail.com

DOI: 10.47750/pnr.2022.13.S01.109

Abstract

Password-based authentication is recognized as insufficient by owners as numerous internet solutions began to influence one another. One Time passwords (OTPs), that may authenticate owners by agreeing about the possession associated with a pre shared benefit, are just about the most favorite possession components within 2 component authentications. 2 component authentications is a popular subcategory of multi factor authentication. The inspiration powering proposing these kinds of structure is treating the little to moderate sizing companies in the concern of deploying an OTP alternative for the authentication of theirs requirements. A present authentication treatment such as just the traditional understanding element is predisposed against numerous community, opportunistic or personalized strikes. In addition, changeover from history methods to superior protection strategies is pricey. Internet qualifications are utilized to recuperate some other qualifications and also intricate strikes are aimed towards the most fragile among most of these internet qualifications. Opposition to OTP replays and also livens strikes, opposition to 3rd party entry, resistance to corrupt insiders, as well as opposition to Denial-of-Service strikes.

Keywords: One Time Password (OTP), Product Security, Authentication Service.

1. INTRODUCTION

Authentication of an end user may be carried out by among the three: expertise, possession, and inherence. When the title proposes, know-how element calls for something which an end user should comprehend to verify the uniqueness. The typical exercise of passwords and typing usernames goes down into this particular group. This method assumes the username is publicly identified and also the password is committed to memory through the person. Authentication is secure so long as the person is definitely the only person who is able to show the password on the program used. Nevertheless, the real life goes through trained us passwords can't be held secure readily as well as the man mind isn't effective at handling numerous passwords for a lot of providers at once. on making use of OTP, that may authenticate owners by agreeing about the ownership associated with a pre collective benefit, are just about the most favorite possession components within 2 component authentication (FA or maybe 2TFA). TFA is a general subgroup of multi factor authentication (MFA). Knowledge element, for training, will be the widely recognized username password pair. As this is essentially the most widely deployed approach to validation, just about all TFA operations consist of this particular feature and also provides among the others. Within the optional method, we've created the multilevel authentication for customer and also the cloud. In addition, the following sections are included in the paper's introduction: Section 2 includes the most recent relevant work on Cloud OTP as a service. Section 3 contains a proposed approach for Multiple Service authentication, Section 4 is a multi-factor authentication implementation, Section 5 is a performance analysis, and Section 6 is the conclusion and feature work.

2. RELATED WORK

Globalization has initiated to increasingly a simple financial as well as radical mutuality, and possesses subdued basic assumptions relating to sovereignty and also the job of nation-state [1].The current authentication as well as critical empathetic pattern for to apply a sensible flash memory card. In order to fulfill the OTP needs, the smart flash memory card is now a decisive gadget, a camera that's popular [2]. In order to lose striking over the usually intangible meaning of the idea of the 'smart city'. Possibly the most newly available variant of Urban Audit material established to be able to measure the elements figuring out the overall performance of serviceable urban centers on OTP concentration [3]. A far more beneficial method is

combining 2 or may be a lot more element authenticator to adore advantages within protection or even hassle-free or possibly each. This will guard us for example from biometric production by altering the end-user specific credential, which is as easy as converting the token that contains the subjective information [4].

Receptors incline to be largely sent out to keep way of a change of difficulties, like material spells, pressure and rapidity through computational measurements and also liveliness has been limited by them. Using the message credits for the Ideal advanced silence to find out the major considerate between the individuals and automated machines. Smart work is a future-oriented work-situation to bring swift business transaction and suitable for users [5]. Using the message credits for the Ideal advanced silence to find out the major considerate between the individuals and automated machines. The Introduction of smart work to the national and external various counties has provided for the users. The primary detached of a password-based genuine crucial exchange protocols is confining the adversary for this situation just [6].

To supply an clear solution for this issue. Systematically check out the usual arguments and also inescapable trade-offs among the look key elements [7]. Defining crucial fashion as well as implying investigation agendas regarding urban areas because they spend money on make new means to be "smart." Identify as well as talk about difficulties, achievement components, as well as impacts of OTP [8]. Through this suggested design the confirmation of Citizen is attained through the tactful setup of electronic signatures, and that is the primary key area of electronic documentation. The recommended software application method type in a deep item-oriented viewpoint and proper access control mechanism is the need of the hour, as the data stored in the cloud needs to be protected securely [9]

A lot of focus has been received by the consumption of public vital encryption to offer protected community communication. Algorithms, as well as categorizations which may be exploited to figure out process protection inside the strategies are provided. The storage capacity can extremely be increased with the use of cloud computing. Cloud computing is a flexible, cost operative and proven delivery platform for providing services. [10].

3. PROPOSED APPROACH

The suggested structure allows suppliers invest much less on OTP based TFA changeover equally within the perspectives of expertise, software, hardware and employers. Furthermore, it allows the subscribers to control a lot of the accounts of theirs effortlessly during a single spot, still by unlikable bookmark profiles. It's thought that outsourcing OTP program inside the cloud might also relieve a lot of cloud program supplier's majority OTP adoption, because they don't need producing extra investment decision. The suggested strategy works well as a 2-component authentication protection mechanism and offers lots of configurable choices by design and style. Consumer bookmark profiles are amenable to potential advancement at giving consumer systems, like targeted password managing, credential control and so on.

3.1 User registration & choose the type of security provider:

In this particular component person has to register underneath the cloud by offering the fundamental specifics. The subsequent registration based upon customer specifics loud will generates just one token as well as send out which token to worker e-mail. Right here right after consumer really wants to confirm the genuineness of his by keying in the legitimate token that was delivered to operator e-mail deal with. In case he goes into completely wrong token the details of his will not take up straight into the cloud. In case consumer goes into the legitimate token he is going to get choices to buy the forms of securities. Following conclusion of protection choice person really wants to do captcha verification as well as cloud OTP verification [11].

3.2 Verify user details & provide the security in cloud:

Here within this component cloud proprietors will own the requests from owners with different kinds of protection choices. Cloud proprietors are going to verify pc user specifics, as well as confirm the scanned documents step. In case they didn't locate appropriate papers and also correct specifics the will drop pc user requests[12]. Special customers UID will probably be create as well as mail it with the end user in case cloud accepts the end user demand. Based upon consumer protection choice consumption may qualified to make use of lengthy specific requirements uses. If he has a high security he is eligible to use all the low level security services.

3.3 Traditional OTP as a Service and Bank account creation:

Within this particular component person has to develop a bank account contained bank account program as well as pour some of the cash directly into bank account. A talk program which entails a conventional protection the end user will be verified by it just at registration period together with the movable number; Cloud can give single verification code on the conventional cloud OTP program [13]. A function to look over the text messages of ours by taping on which specific email are involved by talk software. So we are able to additionally transmit a vocal idea by transforming speech articles to textual content note.

3.4 Secure, Sensitive & Highly Complex:

Grocery retailer is an e commerce grocery store program with protected OTP program. Pc user is able to observe merchandise as well as pour the merchandise directly into cart as well as eliminates the merchandise at cart.

End user may also boost or even reduce the volume of the merchandise inside a cart. This particular commerce program avail protected Fig. 1 Architecture Diagram as well as conventional capabilities all. It is going to ask for opt every single buy. NEFT Transaction is a vulnerable OTP program that has a function to transmit cash to beneficiary bank account to immediately. As well as there's a choice to look at the present bank account harmony.

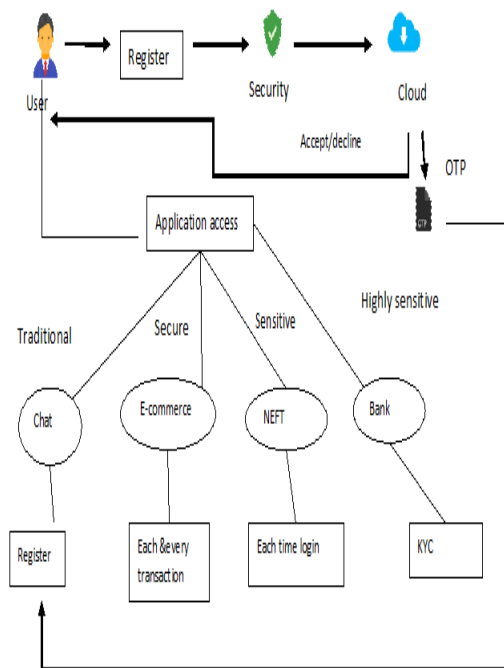


Figure 1: Architecture diagram for multiple service Authentication

This particular commerce program avail protected Figure 1 Architecture Diagram as well as conventional capabilities all. It is going to ask for opt every single buy. NEFT Transaction is a vulnerable OTP program that has a function to transmit cash to beneficiary bank account to immediately. As well as there's a choice to look at the present bank account harmony.

This particular susceptible protection avail all of the functions of outdated and secure OTP program. It is going to ask for opt every single moment of consumer logins to the account of his. Bank software has a function known as internet account development. For this particular person must publish kyc information. In case he currently has cloud bank account under very vulnerable he is able to import all of all those specifics to bank account by distributing cloud services as well as operator UID. In case he provides precise specifics, pc user is able to grab OTP. After conclusion of OTP all of the kyc specifics will likely be brought in to bank account program.

4. IMPLEMENTATION

Online authorizations are used to recover other credentials and composite attacks are directed to the weakest one of many of these online passes. Resistance to OTP replays and livens attacks, resistance to third party access, resistance to corrupt insiders, and resistance to Denial-of-Service attacks. The proposed system lets corporations spend less on OTP-based TFA evolution both in the viewpoints of experience, employers, hardware and software. Moreover, it lets the operators to accomplish many of their accounts easily at one place, yet via unpleasant profiles. It is believed that outsourcing OTP service in the cloud may also prosperity many cloud service providers bulk OTP adoption, as they do not entail making additional investment. The proposed approach is effective as a two factors authentication security mechanism and provides many configurable decisions by design. User profiles are open to forthcoming development at user devices, such as regular password management, credential management etc. There are various Module implementations of multiple service authentications like as

- User registration under cloud & choose the type of security provider
- Verify user details & provide the security in cloud
- Chat Application with traditional OTP as a Service and Bank account creation.
- Grocery with secure, NEFT with sensitive and Bank application with highly sensitive OTP as a Service.

UML Collaboration Diagrams (figure 2) illustrate the relationship and interaction between software objects. They require use cases, system operation contracts and domain model to already exist. The collaboration diagram illustrates messages being sent between classes and objects

4.1. User registration under cloud & choose the type of Security provider

In this module user needs to register under the cloud by providing the basic details. After registration based on user details cloud will generate one token and send that token to user email. Here after user wants to prove his genuineness by entering the valid token which was sent to user email address.

If the enters wrong token his details won't take into the cloud. If user enters the valid token he will get options to choose the types of securities. After completion of security selection user wants to do captcha verification and cloud OTP verification

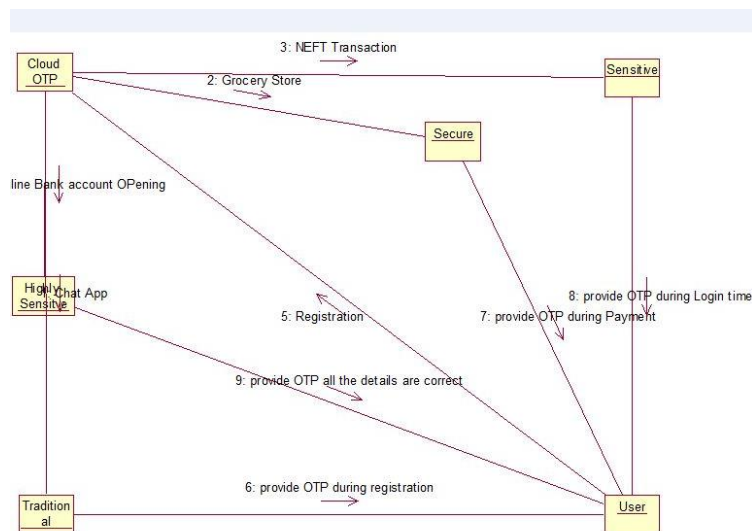


Figure 2: Collaboration diagram of OTP as a service

4.2. Verify user details & provide the security in cloud

Here in this module cloud owners will get the requests from users with various types of security selections. Cloud owners will verify user details, and verify the documents step by step. If they did not find proper documents and proper details they will decline user requests[11]. Unique users UID will be generate and send it to the user if cloud accepts the user request.

Based on user security selection use can eligible to use those particular criteria applications .If he has a high security he is eligible to use all the low level security services.

4.3. Chat Application with traditional OTP as a Service and Bank account creation

In this module user needs to create an account in bank application and add the money into bank. A chat application that involves a traditional security it will verify the user only at registration time with the mobile number; Cloud will give one time verification to the traditional cloud OTP service[12]. Chat application involves an option to read our text messages by tapping on that particular message. And we can also send a voice message by converting voice content to text message.

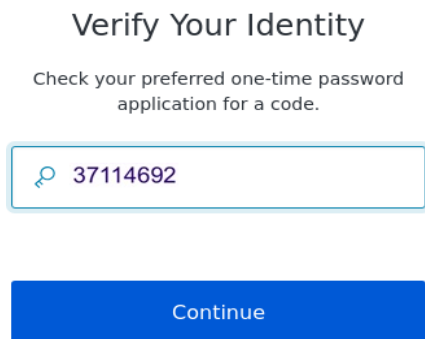


Figure 3 User Login Screenshot

4.4. Grocery store with secure, NEFT transaction with

sensitive and Bank application with highly sensitive OTP as a Service.

Grocery store is an e-commerce supermarket application with secure OTP service. User can see products and add the products into cart and removes the products from cart. User can also increase or decrease the quantity of the products in a cart. This e-commerce application avail secure and traditional features both. It will ask for opt each and every purchase. NEFT Transaction is an sensitive OTP service application which has a feature to send money to beneficiary account to instantly. And also there is a option to check the current account balance[13]. This sensitive security avail all the features of secure and traditional OTP service. It will ask for opt each and every time of user logins to his account. Bank application contains an option called online bank account creation. For this user needs to submit kyc detail. If he already has cloud account under highly sensitive, he can import all those details to bank by submitting cloud service and user UID. If he gives exact details user can get OTP. After completion of OTP all the kyc details will be imported to bank application

Online OTP



Figure 4: Online OTP Creation

Register - OTP

Service name
CloudGate SSO

Account name
demo@example.co.jp

Key (Secret)
5TUXTRKJP7TYNXFJ

Register

Figure 5 OTP Verification

5. EXPERIMENTAL RESULTS

The tests are completed using the TOMCAT 7.0 and MYSQL 5.0 version. The calculations are performed using toolbox that is eagerly available in TOMCAT. In Fig. 3, user login screenshot, here user can give their register account name and key for getting entry into the location created using proposed system. One time password that was twisted to test the computation response in one model as shown in the figure4. Every application access was scheduled with security terms.

The OTP is generated and applied to the Cloud Application is in an output image as shown in the figure 5. The proposed schemes are well trained with the available data and it is widely used for all practices. Some database is kept for training and the rest are kept for testing the proposed schemes. The expected output result has satisfied and achieved the refuge level on associating with the existing model. IN graph Fig 6, Minutes vs lower limit in this proposed system of multiple service authentication .it provides more secure and minimum computation response time.

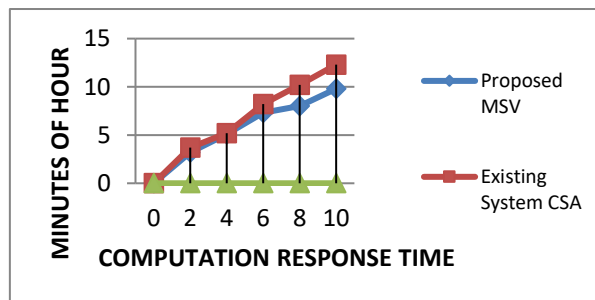


Figure 6 Minutes Vs Computation Response Time

6. CONCLUSION

The dependent authentication systems offerings an OTP for the Cloud-based system provides a to moderate the businesses as well as people to shift the conventional username/password. These authentication systems provide a more protected OTP based TFA plan. A protection as well as secrecy difficulty of migrating the OTP program on the cloud is recognized as very carefully. Attainable imperfections as well as the effects of theirs are talked about. Safety measures & sensible remedies have been claimed. It must be pointed out that the suggested structure doesn't try to resolve the weaknesses of traditional username/password use like learning vulnerability or problem against wondering strikes. In comparison, incorporating another aspect to standard authentication will be the outcome of the above mentioned issues. This's a typical procedure because issues arising against man dynamics are difficult to avoid. A practical use situation is determined along with the attack model of its. The protection requirements having a generic cloud based OTP provision is identified.

REFERENCES

1. Osman, D. A. M. (2019). Two-Factor Authentication and Role-based Access Control for Cloud Services (Doctoral dissertation, Sudan University of Science and Technology). J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
2. ShanmugaPriya, S., Valarmathi, A., & Yuvaraj, D. (2019). The personal authentication service and security enhancement for optimal strong password. *Concurrency and Computation: Practice and Experience*, 31(14), e5009
3. Hlaing, K. S., & Aung, N. A. (2019). Secure One Time Password (OTP) Generation for user Authentication in Cloud Environment.
4. Chan, C. K., & Cheng, L. M. (2000). Cryptanalysis of a remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(4), 992-993.
5. Byun, Y. S., & Kwak, J. (2013). Secure User Authentication Scheme Based on Facial Recognition for Smartwork Environment. *The Journal of Advanced Navigation Technology*, 17(3), 314-325
6. Agarwal, N., Rana, A., & Pandey, J. P. (2019). Guarded dual authentication based DRM with resurgence dynamic encryption techniques. *Enterprise Information Systems*, 13(3), 257-280.
7. Kambou, S., & Bouabdallah, A. (2019, June). A Strong Authentication Method for Web/Mobile Services. In 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 124-129). IEEE
8. Dangi, R., & Pawar, S. (2019). An Improved Authentication and Data Security Approach Over Cloud Environment. In *Harmony Search and Nature Inspired Optimization Algorithms* (pp. 1069-1076). Springer, Singapore
9. Anakath, A. S., Rajakumar, S., & Ambika, S. (2019). Privacy preserving multi factor authentication using trust management. *Cluster Computing*, 22(5), 10817-10823
10. Shinde, M. M. A., & Ramesh, M. J. S. (2019). Authentication in Mobile Cloud Computing. *London Journal of Research in Computer Science and Technology*, Volume 19 | Issue 3 | Compilation 1.0
11. Dwi Ely Kurniawan, Mohd Iqbal Friad (2021), Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance, *Journal of Physics Conference Series*, doi:10.1088/1742-6596/1783/1/012041
12. Shakir M. H. Al-Faraj, Huda K. Saadeh, One Time Password Generation based on Random Permutation using User Identity with Timestamp (2021), *International Journal of Engineering and Advanced Technology (IJEAT)* ISSN: 2249 – 8958 (Online), Volume-9 Issue-4
13. Emir Erdem and Mehmet Tahir Sandikkaya (2018), OTPaaS —One Time Password as a Service, *IEEE Transactions on Information Forensics and Security*, 14(3):1-1
14. Dwi Ely Kurniawan, Dwi Ely Kurniawan (2019) Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance, *Journal of Physics Conference Series* 1783(1):012041
15. Kyaw Swar Hlaing | Nay Aung Aung (2019), Secure One Time Password (OTP) Generation for user Authentication in Cloud Environment, *Volume 6, Issue 3*