e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

OTP VERIFICATION BY PHP USING TEXTLOCAL

Avdhesh Kumar*1, Abhishek Kumar Jha*2, Mr. Abhist Kumar*3

*1,2Student, Department Of Computer Science And Engineering, GALGOTIAS UNIVERSITY, Noida, UP, India.

*3Assistant Professor, Department Of Computer Science And Engineering, GALGOTIAS UNIVERSITY, Noida, UP, India.

ABSTRACT

This paper describes the process "a secure payment system using a face recognition method" - a project designed. It explains the main purpose of the project which is to be able to develop a secure and secure payment system using face recognition in the Python program language with the help of OpenCV. It uses the confidence level that can be defined as the value generated by the system that informs the accuracy of the forecast. This project is made by combining various visual modules with a pattern mirror. In this project the various existing methods are put together to give us the result. A one-time PIN and password (OTP) are used for security measures to make the job safer and more efficient. OTP will be sent to the user's registered phone number. Physician certification in online medical questionnaires is very important because users may be misled by incorrect disease predictions or related suggestions and that may create dangerous situations. Here, we have introduced a Doctor-Validation Strategy (DVS) with Python system to easily verify such credentials or information for doctors who sign up for online medical query systems. This strategy allows the administrator / developer to verify the doctor by certifying certificates, proof of ID and mobile phone number through the OTP verification process, before authorizing registration. As Python is an advanced, flexible and easy-to-use programming language, we have developed our Doctor Authenticator system in the Python platform Currently there are two voting systems in India. Votes are secret and electronic voting machines, but these two processes have limitations or inconsistencies. The current system is also not secure. Many people miss out on the opportunity to vote simply because they need to go to the polls and wait in large numbers to vote. In this paper, we have suggested a way to vote. In our approach, the voting process has three stages of security. The first stage is face recognition, the second stage is Verification ID number (EID), and the third stage is One-Password (OTP) verification using the user's registered phone number. The electronic voting machine is already advanced and widely used in many developed countries. But most of them use facial expressions. In developing countries RFID per capita is not available. And using RFID is still a valuable solution. to address these issues we have developed this project where the PC will be used as a host. This computer has the ability to process images and control the entire voting system. The camera will be used to take a photo of the citizen's face identification that this user is a valid voter of that region. If the citizen is legal and the person will be allowed to cast their vote. Each vote was saved in a text file format. At the end of the voting period that data will be processed by an authorized voting officer via OTP. Device lifecycle management intellectual property (IP) is used to adjust the standard register transfer rate (RTL) based on customer requirement instead of designing multiple designs of different specifications. In this work, the standard test benchmark of universal verification methodology (UVM) is written to verify the IP life cycle control of the device and the text can automatically generate a specific verification location provided by an excel sheet instead of creating separate verification areas for different IPs. . The UVM-based verification platform is designed to verify inventory due to its rich class libraries, categories, UVM industry, reporting system, metaprogramming etc. on all other verification methods. In this work, a UVM-based verification bench for all IP blocks is written and simulation is verified using cadence ncsim, code coverage is analyzed using an integrated cadence metrics center.

I. INTRODUCTION

We live in a fast-paced world and most of us are very aware of time. People were using all the technologies like internet, cell phones, cooking / cleaning or other household appliances, car motors etc. in their daily lives to save their time. Similarly, to save time, people use various online resources for their daily needs such as shopping, paying bills, banking, booking a hotel / hotel, ordering food etc. skepticism so that they can avoid large lines and direct physician consultation procedures [1-3]. But unfortunately the information from many

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

medical questionnaires is unreliable due to the absence or improper verification of the doctor as well. This can cause serious problems for users physically and mentally. Therefore, the developers / managers of online medical questionnaires should ensure the care that is most important in ensuring physicians who enroll in their programs. And people should know the procedures for reassuring a doctor about a site they are discussing with their health-related concerns. We demonstrated a series of medical questions based on NLP tools and published that work recently [6]. Then, in an effort to address the aforementioned problem, we developed a Doctor-Validation-Strategy (DVS) to properly certify physicians for their enrollment in our program. While developing any program, the choice of its planning platform is very important. Proper selection of the planning platform will provide excellent comfort and results. Here we have used Python's planning platform to improve Doctor Validation-Strategy (DVS). Studies show that Python is the fifth most popular language. Python has a large number of general public libraries that provide many tools that allow you to perform many tasks with great ease. Moreover, when compared to other languages, Python only needs to be coded with minimal and easy to do many such things [7, 8]. Electronic voting is the most common way to control elections using Electronic Voting Machines, sometimes called "EVMs". Prior to the introduction of electronic voting, India used ballot papers and counting. The ballot paper system was widely criticized for fraudulent voting and booting, in which party members of the party took the ballot boxes and stuffed them with fake pre-filled ballots. Printed ballot papers are also expensive, requiring a lot of resources after voting to count hundreds of millions of votes individually. EVM embedded features such as electronically limiting the voting rate to five per minute. India's EVMs are autonomous machines built with one-click, memory-only memory. They do not have wireless or cable internet components and a visible connector. The M3 version of EVM includes the VVPAT system. With these problems in mind we created this project where the raspberry pi will be used as a host.

II. METHODOLOGY

Various TOKEN CONCEPT

Dynamic Mobile Token has a vision for online trading. Portable Token turns into an additional part of the verification cycle, to indicate that the client performing the login meeting or exchange process is the real client.

Verification strategy

Verification point to show that user access is a real user. There are many strategies that can show you, however, verification strategies can be seen visually in three stages of strategy:

• What You Know It is a common verification strategy. This process relies on data privacy, such as PIN. This process decides that no one does the mystery unless it is a real user.

• Something You Have This is usually the default feature to trigger secure authentication. This strategy relies on generally notable features, for models, attractive card / smartcard, machine tokens, USB tokens, and more. This strategy simulates that no one has the tools other than the actual one you use.

• Something You Are This is the most inconsistently used strategy due to innovation and the human element too. This technique depends on the uniqueness of the body parts that isn't stay alive in others like finger impression, voice, retina or finger view. This procedure measures the parts of the body, for example, the fingerprints and the retina differently.

Secret key Mode:

Dynamic Mobile Token there are two mode utilized:

Challenge / Response Mode (C / R): This mode is frequently used during rotations. In this mode the server provides testing as a continuation of numbers. That number must be entered into the Mobile Token in order to obtain a solution (duplication). Then, at that point, the user enters the number from his or her Mobile Token in the text box on the site. Portable Token will provide another code however with the same code challenge. Reliance from time to time when we answer a test with a token.

Built-in Mode (Answer Only): In this mode the server does not provide any critical value (challenge). Versatile Token clients can directly provide continuity of a combination of numbers and letters without having to enter the test. As with C / R mode, the Mobile Token is assigned a variety of codes from time to time depending on when the token is strictly instructed to forward the codes it generated.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

SECURITY RATE

In the real level of security in C / R mode and Self Generated (Answer Only) is the only password again. However, unlike the password used for login, passwords from Mobile Token are restricted for security, specification:

Only Once: Once a secret phrase has been used, the same password cannot be used the next time. As such, there is no good reason to hold rejected passwords on Mobile Token on the grounds that the secret key cannot be reused. Regardless of the possibility, it is assumed that the private key is considered to be able to block access to the server, it is still an important secret statement as the server's secret phrase has never been used.

Can only be used within a limited time: Mobile token created passwords with a limited life span, which can be within 2-3 minutes. At the end of the year, the password will no longer be used, despite the fact that it has never been used before. Time is the most important part of this Mobile Token program.

Only Use in Small Theme: If a private key / PIN is used - login is a free private setup, as is the case with a non-existent key but, it can do a lot of things, from seeing the fix, look really good. in trade and so on. However, a token generated by a secret key should be used in a limited way, for example, the secret key used to purchase the appropriate representative number 08123456789, cannot be used to move the archives.

III. MODELING AND ANALYSIS

GENERAL DESIGN SYSTEM

Authentication Process

For example, passwords as a rule, provided that the verification is successful, the password sent out by the customer is incompatible with the passwords stored on the server. For security reasons the server does not usually store user passwords in plain text format. Normally, the server stores user passwords in a hash format so that it cannot be recovered with a blank text format. Therefore the effective validation value can be defined as the result of the hash calculation of the secret phrase sent by the customer should be incomprehensible to the hash value placed on the server. (Figure 1)

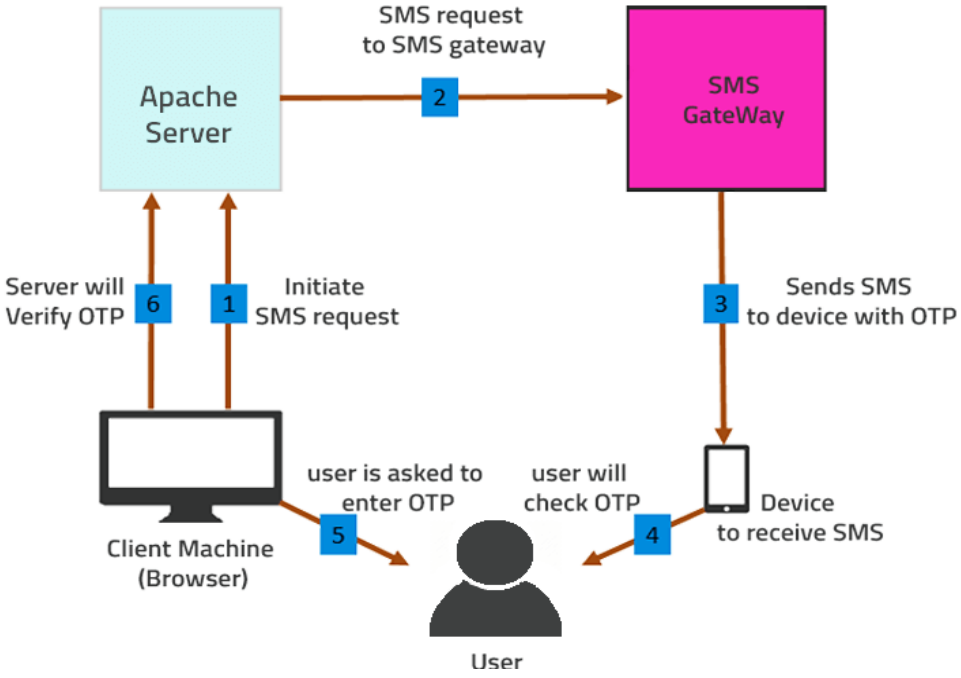
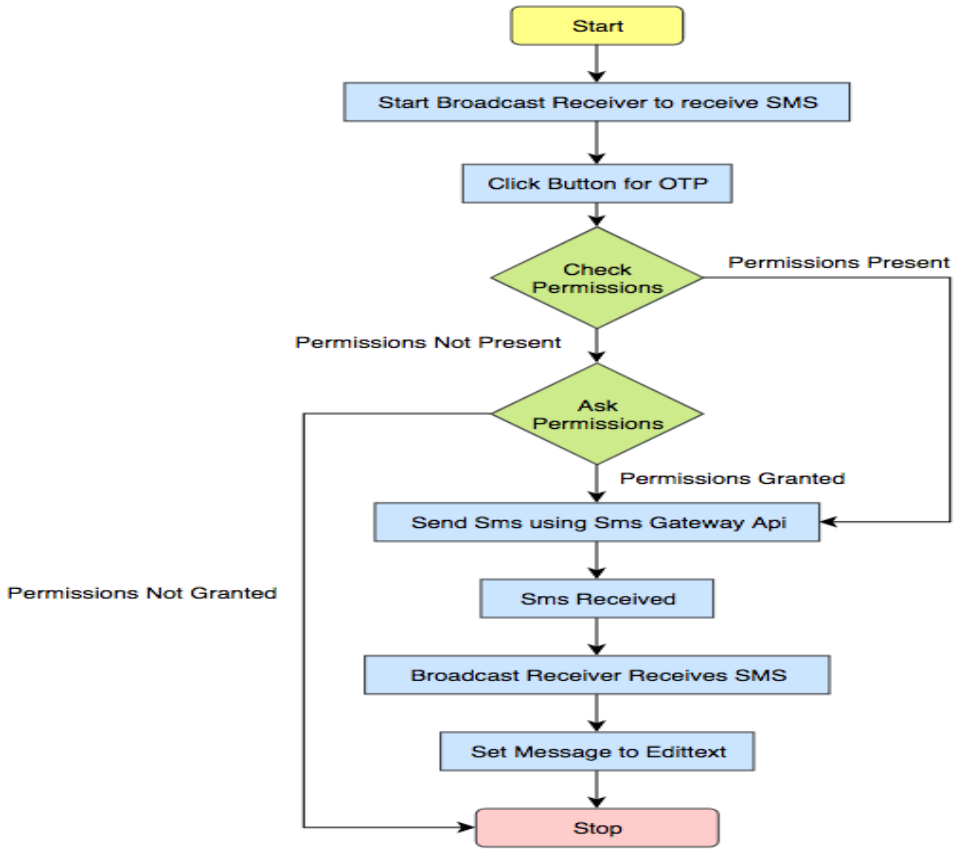


Figure 1: Hash Password Authentication Process

The Versatile Token Verification course on the server has very important time certificates. Clients need to connect the clock to the phone and the clock on the server, the difference in authorized hours is less than 3 minutes and more than 3 minutes, more than that is considered incorrect or code is used. The cycle of a series of interactive framework between server, customer, employee, Mobile Token, and site has strong relationships and cannot be separated. In view of the crash of one frame, another series cannot be started or managed (see Figure 2).

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

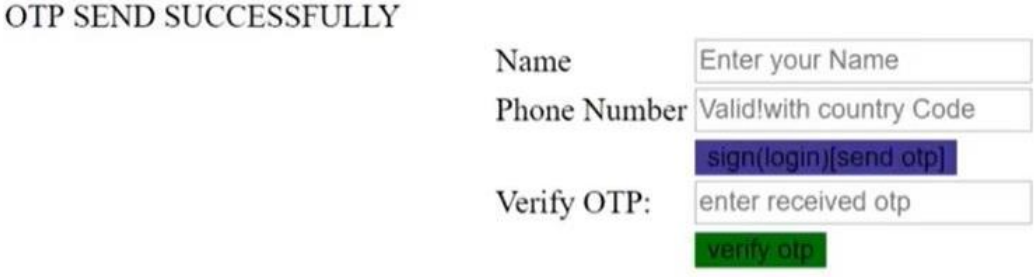


IV. RESULTS AND DISCUSSION

Project Design:

Presently we should follow the means referenced above by utilizing Python to make an application for the assignment of OTP check. I will begin by bringing in the essential Python library that we really want for this undertaking:

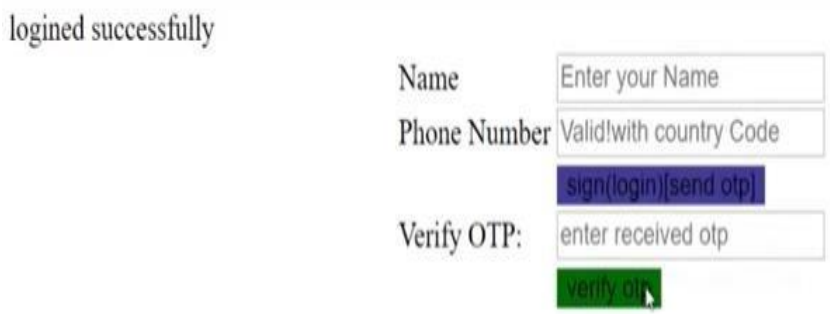
Presently I will produce an irregular number and store it in a variable which I will utilize while sending message to the clients.



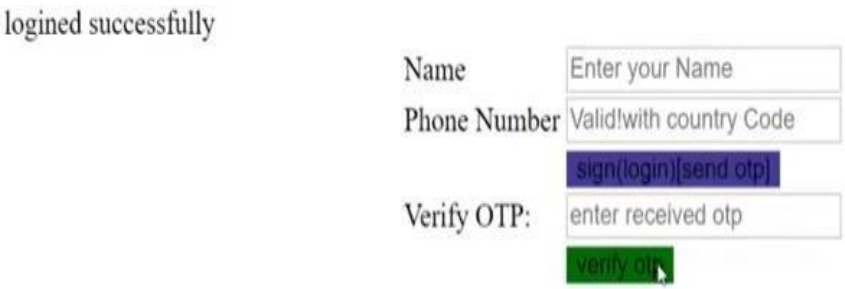
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

Presently, before we go on, you really want to have your Google application secret phrase to have the option to send messages utilizing your Gmail account. After you make your application secret phrase for your Gmail account you will get a key.

Duplicate that key and glue in the codeunderneath to send messages for OTP check utilizing Python:



OUTPUT:



V. CONCLUSION

Throughout the research conducted here, it is thought that the One time password is an integral part of each business environment. This paper concludes with regard to strategies for creating a secret age-old framework and the Trojan impact on the framework. Throughout the research conducted here, it is thought that the One time password is an integral part of each business environment. This paper concludes with regard to strategies for creating a secret age-old framework and the Trojan impact on the framework. Today, not only mailing agents and banking sector need to worry about the security of their OTPs. All the companies from various sectors and sizes make use of OTP for authenticating their clients to access the available resources in a user-friendly way in the present cut-throat business environment. Therefore, there is a need to develop a user-friendly and secure OTP generation process and one such model has been presented in this study. This model generates OTP using the hardware and software profiles of the user device as the initial seed. The OTP generated can be transmitted to the users by means of email, push message, etc. Work One-Time Passwords are a leading technology in today ' s Two-factor Authentication Systems for more secure applications. We developed a two-factor authentication prototype for mobile phones using this OTP calculation. The prototype was used in practice for a year and provided complete protection against replay attacks and detection of forced delay attacks. The implementation had the advantage of simple onepass authentication message exchange, no need for a third party, low computation cost and no cost for proprietary tokens. However, using a mobile phone as the OTPs generator has vulnerabilities to keyboard monitor attacks, memory scan attacks and software clone attacks. We will try to counter these threats in future research.

VI. REFERENCES

[1] "Real Time Face Detection and Tracking Using OpenCV", Prof. P Y Kumbhar, Mohammad Attaullah, Shubham Dhere, Shivkumar Hipparagi INTERNATIONAL JOURNAL FOR RESEARCH IN EMERGING SCIENCE AND TECHNOLOGY, VOLUME-4, ISSUE-4, APR-2017 E-ISSN: 2349-7610,

[2] "Facial Recognition using OpenCV", Shervin Emami,Valentin Petru! SUCIU Senior Systems Software Engineer Mobile Computer Vision Team, NVIDIA AUSTRALIA IT&C Security Master Department of Economic Informatics and Cybernetics Bucharest University of Economic Studies ROMANIA, "Multiple

Face Detection and Tracking using Adaboost and Camshift Algorithm", Mr.Ashwith Kumar S. K., Dr. Suresh D., Mr. Sanjeev Kubakaddi,

[3] Image-based Face Detection and Recognition: "State of the Art"", Faizan Ahmad, Aaima Najam and Zeeshan Ahmed,

[4] "Biometric Face Recognition PaymentSystem", Surekha. R.Gondkar,

[5] Nikita Bakshi and VibhaPrabhu, "Face recognition system for access control using principal component analysis", 2017 International Conference On Intelligent Communication And Computational Techniques(ICCT), Manipal University Jaipur, Dec 22-23,2017,

[6] Chinchu S., Anisha Mohammed and Mahesh B. S., "A Novel Method for RealTime Face Spoof Recognition for Single and Multi-User Authentication",2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT).

[7] Dileepkumar and Yeonseungryu, "A Brief Introduction of Biometric and Fingerprint Payment Technology", 2008 Second International Conference on Future Generation Communications and Networking Symposia.

[8] Dileepkumar, Dr. Yeonseungryu and Dr.Dongseop Kwon, "A Survey on Biometric Fingerprint: TheCard less Payment System", 2008 Second International Symposium on Biometrics and Security Technologies,

[9] "Multilayer Image Segmentation Based on Gaussian Weighted Euclidean Distance and Nonlinear Interpolation", 2017 10th International Congress on Image and Signal Processing, Biomedical Engineering andInformatics (CISP-BMEI 2017)

[10] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", 4th Edition, Pearson Education Inc, 2018,

[11] Rafael C.Gonzalez, Richard E. Woods and Steven L. Eddins, "Digital Image Processing using MATLAB", 2nd Edition TataMcgraw hill education pvt.Ltd.

[12] Hung-Yuan Cheng, Chun- Cheng Hou, Shou-Jyun Liang, "Face Detection and Posture Recognition in a Real Time Tracking System", 2017 IEEE International Systems Engineering Symposium(ISSE)

[13] Maria petrou and costas petrou, image processing: the fundamental, 2nd edition, Wiley publications,

[14] M. Turk and A. Pentland, Eigen faces for Recognition, Journal of cognitive Neuroscience vol. 3, no. 1, pp. 71–86, 1991.

[15] Varthika Mehta and Deepak Punetha, A Fascinating Territor Approaching Edge Detection using Feasibility of Eigen faceto Identify an Individual, 2015 2nd International Conference on Advances in Computing and communication engineering.