iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IX **Month of publication:** September 2020

DOI: https://doi.org/10.22214/ijraset.2020.31435

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IX Sep 2020- Available at www.ijraset.com

Enhanced E-Commerce Application Security using Three Factor Authentication

Dr. Sajeev J[1], Anuja Jacob[2], Dr. Mahalekshmi[3]
[1]*Head of Department MCA,* [2]*Final Year MCA,* [3]*Principal, Sree Narayana Institute of Technology, Kollam, Kerala*

Abstract: ***As we all know that e-commerce playing an inevitable role in our day to day life. As much as technology makes things easier for us, it makes ourselves open to online attacks. For online transactions, all we have to do is login to our account and do the transaction. Currently, financial sites use static passwords, which are easier for customers to use. These may lead to the user's account into risk. Given enough time and number of attempts, an attacker can easily access login. Static passwords can be vulnerable to attacks such as shoulder-surfing, dictionary attacks and so on. By constantly altering the password, as is done with a one time password, this risk can be greatly reduced[4]. We propose a system with different authentication methods for targeting online financial websites. E-Commerce applications use OTP to provide security by changing the password every time, so OTP is preferred. For a personal recognition biometric techniques can be used. Unlike other biometric, fingerprint is unique. Noisy password is a strong alternative for static password. Hence, we are trying to incorporate a combination of all the three to provide a secure method to perform E-transaction in E-Commerce applications.***
Keywords: dlib algorithm

I. INTRODUCTION

Three-factor authentication is mainly used in businesses and government agencies that require high degrees of security. In this paper, 'Enhanced e-commerce application security using three factor authentication' we introduced three different authentication methods. They are password, OTP and face recognition. It is important to know that the reliability of authentication is affected not only the number of factors involved but also how they are implemented. In each category, the choices made for authentication rules greatly affect the security of each factor. Poor or absent password rules, for example, can result in the creation of passwords like "guest," which completely defeats the value of using a password. Best practices include requiring inherently strong passwords that are updated regularly. Facial recognition systems can in some cases be defeated by holding up a picture. More effective systems may require a blink or even a wink to register. Lax rules and implementations result in weaker security; alternatively, better rules can yield better security per factor and better security overall for multifactor authentication systems.

In this application, the user can access the system only by successfully completing the three step authentication. When a customer register the site, he must enter the name, password, phone number and his face image is taken from the web camera. After registering , he can logon to the system only by the following steps. First ,he must enter the password and the password is authenticated. He can go to next step only if the password is correct. Second step is he must enter the OTP which is send to the registered mobile number. Third step is face recognition. Face recognition is done using the dlib library algorithm.

II. BACKGROUND

A. Technologies used in this Project

1) Python is a simple, general purpose, high level, and object-oriented programming language. Python is an interpreted scripting language also. Guido Van Rossum is known as the founder of python programming. Python is a general purpose, dynamic, high level, and interpreted programming language[1]. It supports Object Oriented programming approach to develop applications. It is simple and easy to learn and provides lots of high-level data structures. Python yet powerful and versatile scripting language, which makes it attractive for Application Development. Python's syntax and dynamic typing with its interpreted nature make it an ideal language for scripting and rapid application development.

2) Django Web Framework is a free and abides by the MVT (Model View Template) pattern. It is maintained and authorized by the Django Software Foundation (DSF) which is an independent organization established firmly as a non-profit foundation.

Django's primary most goal is to simplify the creation of complex websites which are also data-driven ones. Django emphasizes much on reusability of components, lessening codes, lowering coupling, rapidity in development, etc[2]. Python is used incessantly in most of the tasks, including file settings and data models. Django also provides a voluntary administration to create, read, update and delete the interface that is generated through introspection and further configured by admin models.

III. EXISTING SYSTEM

A. How it Actually works

In the existing system, only two factor authentication method is provided. So the user's account into risk. Currently, financial sites use static passwords, which are easier for customers to use. These can also potentially put the user's account into risk. Given enough time and number of attempts, an attacker can easily access login. Static passwords can be vulnerable to attacks such as shoulder-surfing, dictionary attacks and so on.

B. Drawbacks of the existing system

1) *Surfing Attack:* Also known as peeping attacks. An attacker can gain access to the account or a session by observing the logging activity of the actual user by either using a camera to observe the keys entered or by peeping over the shoulder.
2) *Dictionary Attack:* An attack used to breach a password protected system by systematically entering the words in dictionary as password.
3) *Guessing Attack:* An attack achieved by attempting guesses of password using personal information of the user such as mobile number, pet's name.

IV. PROPOSED SYSTEM

A. Description

1) Proposed system has three phase of authentication method. They are:
2) Password
3) OTP
4) Face Recognition

During the Enrollment phase, each user should enroll by providing their personal information along with their password and face image. Face image would be collected using web camera. These samples would be filtered. The features such as minutiae, orientation would be extracted and a template would be created. This template would be stored in the database along with the user's other details. Enrollment phase is followed by the authentication phase, where the user enters his or her noisy password and face image input into the recognition system, which is further feature extracted and matched with the sample from the Database. Upon successful matching, the OTP is generated. This OTP should be sent to the user through secure communication. This is secure communication can be achieved by using the commonly used public key cryptography- Elliptic Curve cryptography (ECC). Only by entering the OTP that the user received, the e-transaction will be successful.

B. Algorithm Used

1) *Dlib Library Algorithm:* Dlib is a powerful library having a wide adoption in image processing community similar to OpenCV[9]. Researchers mostly use its face detection and alignment module. Beyond this, dlib offers a strong out-of-the-box face recognition module as well. Even though it is written in c++, it has a python interface as well.

V. RESULTS AND DISCUSSION

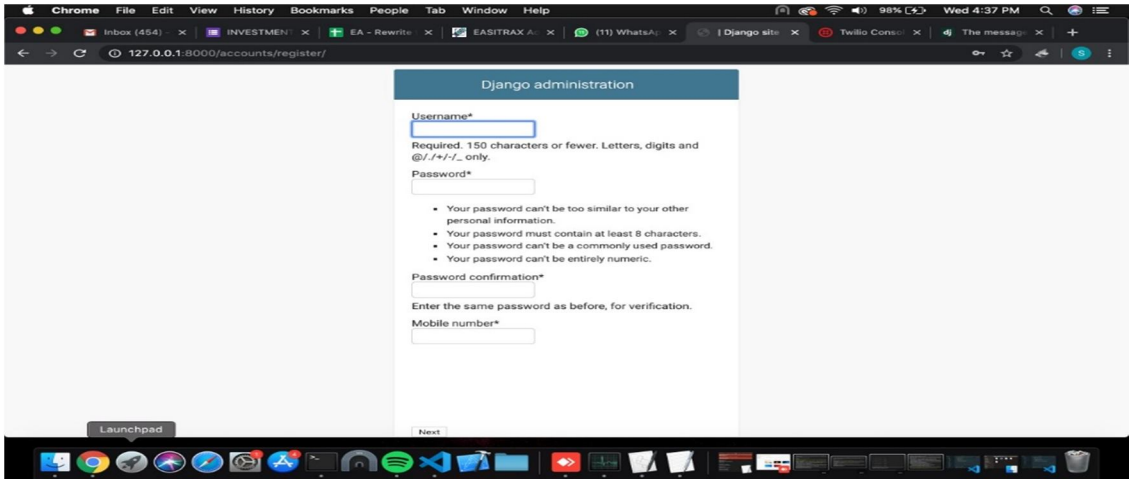


Fig 1:Customer registration

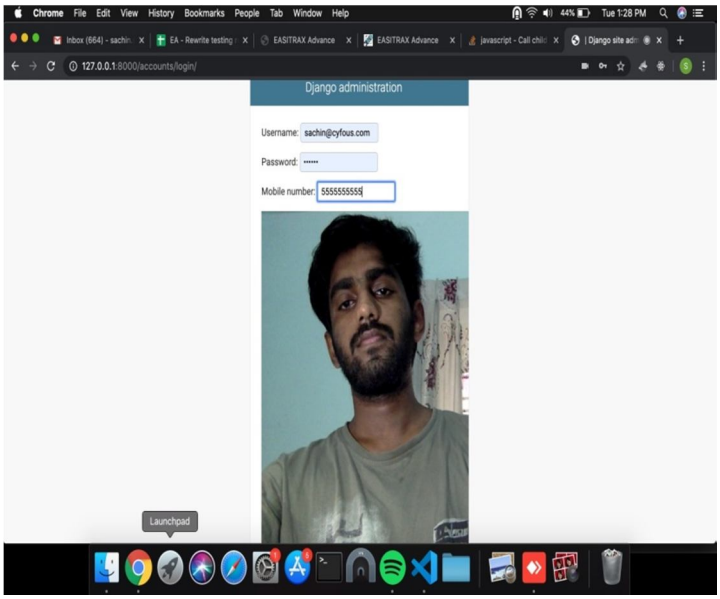


Fig 2: Login page

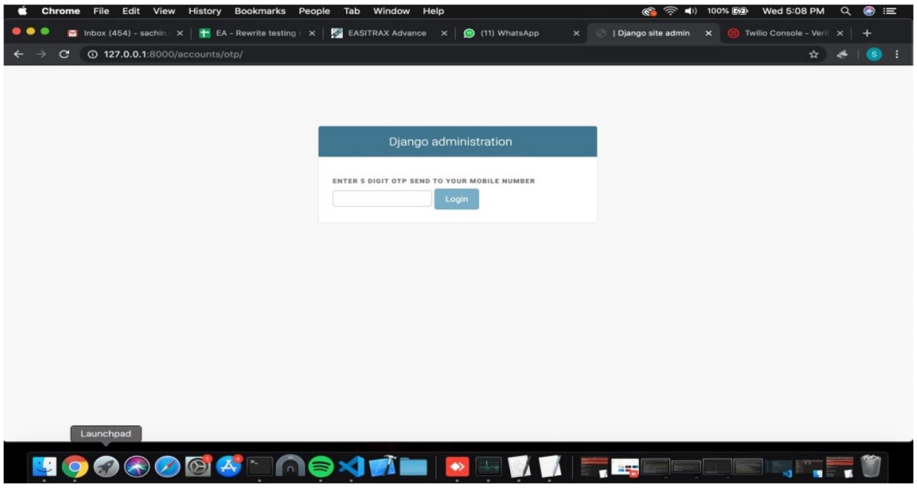


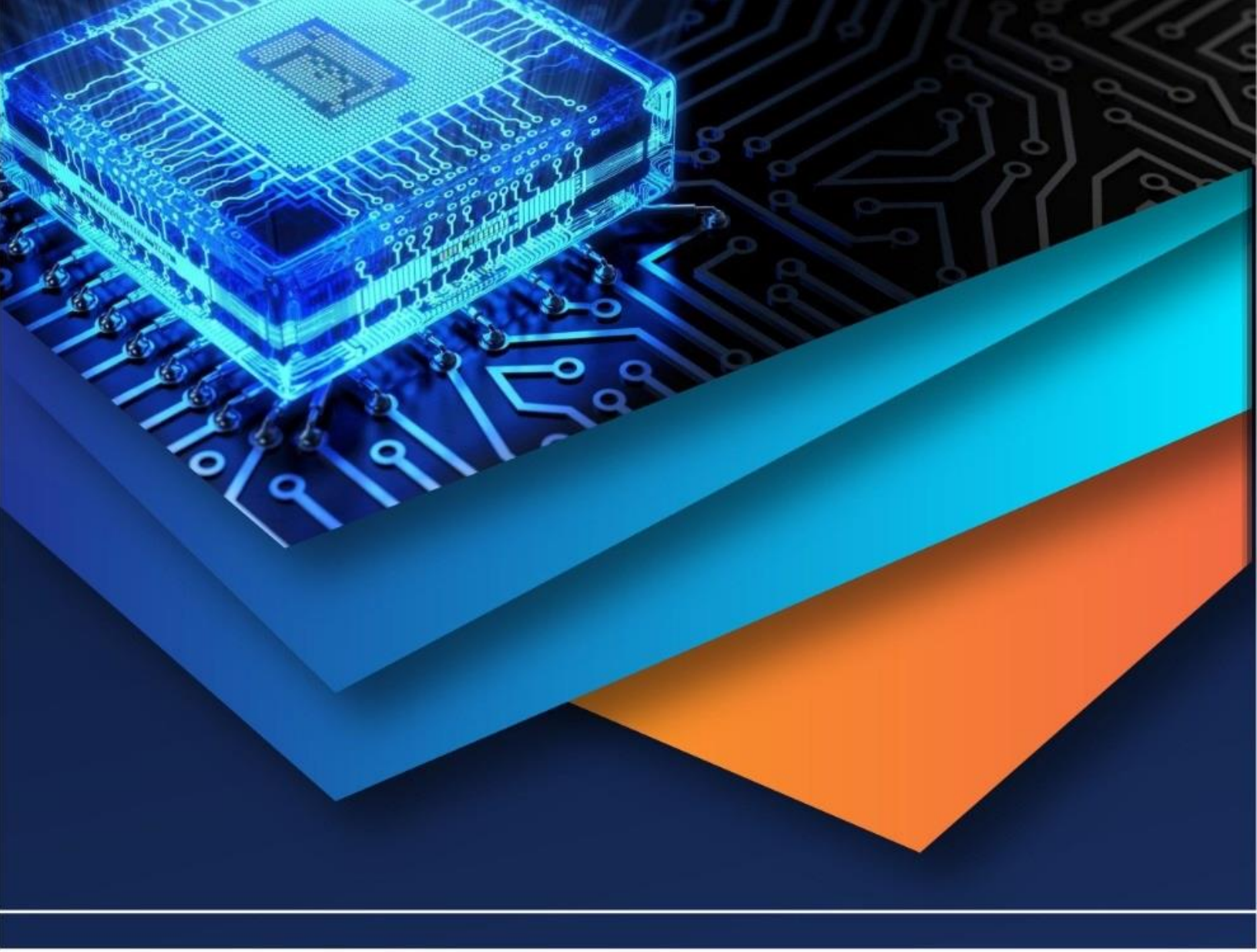
Fig 3: OTP verification

VI. CONCLUSION

Currently, financial sites use static passwords, which are easier for customers to use. These can also potentially put the user's account into risk. Given enough time and number of attempts, an attacker can easily access login. Static passwords can be vulnerable to attacks such as shoulder-surfing, dictionary attacks and so on. By constantly altering the password, as is done with a one time password, this risk can be greatly reduced. We propose a system with a different perspective of password security targeting online financial websites. E-commerce applications use OTP to provide security by changing the password every time, so OTP is preferred. For a personal recognition face image is used. So it ensure more security.

REFERENCES

[1] Django for Beginners: Build websites with Python and Django
[2] Agile Software Development, Principles, Patterns, and Practices- Robert C. Martin
[3] Research Article Access to Network Login by Three-Factor Authentication for Effective Information Security.
[4] https://pypi.org/project/face-recognition/
[5] https://www.w3schools.com/django/
[6] https://www.w3schools.com/python/
[7] https://docs.djangoproject.com/en/3.1/topics/install/
[8] https://www.geeksforgeeks.org/python-multiple-face-recognition-using-dlib/
[9] https://www.analyticsvidhya.com/blog/2018/08/a-simple-introduction-to-facial-recognition-with-python-codes/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY