A USER-CENTRIC MACHINE LEARNING FRAMEWORK FOR CYBER SECURITY OPERATIONS CENTER

TABLE OF CONTENTS

ABSTRACT

In order to ensure a company's Internet security, SIEM (Security Information and Event Management) system is in place to simplify the various preventive technologies and flag alerts for security events. Inspectors (SOC) investigate warnings to determine if this is true or not. However, the number of warnings in general is wrong with the majority and is more than the ability of SCO to handle all awareness. Because of this, malicious possibility. Attacks and compromised hosts may be wrong. Machine learning is a possible approach to improving the wrong positive rate and improving the productivity of SOC analysts. In this article, we create a user-centric engineer learning framework for the Internet Safety Functional Center in the real organizational context. We discuss regular data sources in SOC, their work flow, and how to process this data and create an effective machine learning system. This article is aimed at two groups of readers.

The first group is intelligent researchers who have no knowledge of data scientists or computer safety fields but who engineer should develop machine learning systems for machine safety. The second groups of visitors are Internet security practitioners that have deep knowledge and expertise in Cyber Security, but do Machine learning experiences do not exist and I'd like to create one by themselves. At the end of the paper, we use the account as an example to demonstrate full steps from data collection, label creation, feature engineering, machine learning algorithm and sample performance evaluations using the computer built in the SOC production of Seyondike.

LIST OF FIGURES

1. INTRODUCTION

1.1 Brief Information

Cyber security incidents will cause significant financial and reputation impacts on enterprise. In order to detect malicious activities, the SIEM (Security Information and Event Management) system is built in companies or government. The system correlates event logs from endpoint, firewalls, IDS/IPS (Intrusion Detection/Prevention System), DLP (Data Loss Protection), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), Windows/Unix security events, VPN logs etc. The security events can be grouped into different categories.

The logs have terabytes of data each day. From the security event logs, SOC (Security Operation Center) team develops so-called use cases with a pre-determined severity based on the analysts experiences. They are typically rule based correlating one or more indicators from different logs. These rules can be network/host based or time/frequency based. If any pre-defined use case is triggered, SIEM system will generate an alert in real time. SOC analysts will then investigate the alerts to decide whether the user related to the alert is risky (a true positive) or not (false positive). If they find the alerts to be suspicious from the analysis, SOC analysts will create OTRS (Open Source Ticket Request System) tickets. After initial investigation, certain OTRS tickets will be escalated to tier 2 investigation system (e.g., Co3 System) as severe security incidents for further investigation and remediation by Incident Response Team. However, SIEM typically generates a lot of the alerts, but with a very high false positive rate. The number of alerts per day can be hundreds of thousands, much more than the capacity for the SOC to investigate all of them.

Because of this, SOC may choose to investigate only the alerts with high severity or suppress the same type of alerts. This could potentially miss some severe attacks. Consequently, a more intelligent and automatic system is required to identify risky users. The machine learning system sits in the middle of SOC work flow, incorporates different event logs, SIEM alerts and SOC analysis results and generates comprehensive user risk score for security operation center. Instead of directly digging into large amount of SIEM alerts and trying to find needle in a haystack, SOC analysts can use the risk scores from machine learning system to prioritize their investigations, starting from the users with highest risks. This will greatly improve their efficiency, optimize their job queue management, and ultimately enhance security, Specifically, our approach constructs a framework of user centric machine learning system to evaluate user risk based on alert information. This approach can provide security analyst a comprehensive risk score of a user and security analyst can focus on those users with high risk scores. To the best of our knowledge, there is no previous research on building a complete systematic solution for this application. The main contribution of this paper is as follows: x An advanced user-centric machine learning system is proposed and evaluated by real industry data to evaluate user risks. The system can effectively reduce the resources to analyze alerts manually while at the same time enhance enterprise security. x A novel data engineering process is offered which integrates alert information, security logs, and SOC analysts investigation notes to generate features and propagate labels for machine learning models.

1.2 Motivation

we present a user-centric machine learning system which leverages big data of various security logs, alert information, and analyst insights to the identification of risky user. This system provides a complete framework and solution to risky user detection for enterprise security operation center

1.3 Objective

we use the system we built in the Symantec SOC production environment as an example to demonstrate the complete steps from data collection, label creation, feature engineering, machine learning algorithm selection, model performance evaluations, to risk score generation

1.4 Problem Statement

Most approaches to security in the enterprise have focused on protecting the network infrastructure with no or little attention to end users. As a result, traditional security functions and associated devices, such as firewalls and intrusion detection and prevention devices, deal mainly with network level protection. Although still part of the overall security story, such an approach has limitations in light of the new security challenges described in the previous section.

Data Analysis for Network Cyber-Security focuses on monitoring and analyzing network traffic data, with the intention of preventing, or quickly identifying, malicious activity. Risk values were introduced in an information security management system (ISMS) and quantitative evaluation was conducted for detailed risk assessment. The quantitative evaluation showed that the proposed countermeasures could reduce risk to some extent.

Investigation into the cost-effectiveness of the proposed countermeasures is an important future work. It provides users with attack information such as the type of attack, frequency, and target host ID and source host ID. Ten et al. proposed a cyber-security framework of the SCADA system as a critical infrastructure using real-time monitoring, anomaly detection, and impact analysis with an attack tree-based methodology, and mitigation strategies

2. SYSTEM ANALYSIS

2.1 Existing System

Most approaches to security in the enterprise have focused on protecting the network infrastructure with no or little attention to end users. As a result, traditional security functions and associated devices, such as firewalls and intrusion detection and prevention devices, deal mainly with network level protection. Although still part of the overall security story, such an approach has limitations in light of the new security challenges described in the previous section.

Data Analysis for Network Cyber-Security focuses on monitoring and analyzing network traffic data, with the intention of preventing, or quickly identifying, malicious activity. Risk values were introduced in an information security management system (ISMS) and quantitative evaluation was conducted for detailed risk assessment. The quantitative evaluation showed that the proposed countermeasures could reduce risk to some extent. Investigation into the cost-effectiveness of the proposed countermeasures is an important future work. It provides users with attack information such as the type of attack, frequency, and target host ID and source host ID. Ten et al. proposed a cyber-security framework of the SCADA system as a critical infrastructure using real-time monitoring, anomaly detection, and impact analysis with an attack tree-based methodology, and mitigation strategies.

Disadvantage Of Existing System

- Firewalls can be difficult to configure correctly.
- Incorrectly configured firewalls may block users from performing actions on the Internet, until the firewall configured correctly.
- Makes the system slower than before.
- Need to keep updating the new software in order to keep security up to date.
- Could be costly for average user.
- The user is only constant.

2.2 Proposed System

User-centric cyber security helps enterprises reduce the risk associated with fast-evolving end-user realities by reinforcing security closer to end users. User-centric cyber security is not the same as user security. User-centric cyber security is about answering peoples' needs in ways that preserve the integrity of the enterprise network and its assets. User security can almost seem like a matter of protecting the network from the user — securing it against vulnerabilities that user needs introduce. User-centric security has the greater value for enterprises. cyber-security systems are real-time and robust independent systems with high performances requirements. They are used in many application domains, including critical infrastructures, such as the national power grid, transportation, medical, and defense. These applications require the attainment of stability, performance, reliability, efficiency, and robustness, which require tight integration of computing, communication, and control technological systems.

Critical infrastructures have always been the target of criminals and are affected by security threats because of their complexity and cyber-security connectivity. These CPSs face security breaches when people, processes, technology, or other components are being attacked or risk management systems are missing, inadequate, or fail in any way. The attackers target confidential data. Main scope of this project in reduce the unwanted data for the dataset.

Advantages Of Proposed System

- Protection against data from theft.
- Protects the computer from being hacked.
- Minimizes computer freezing and crashes.
- Gives privacy to users.
- Securing the user-aware network edge.
- Managing user-centric security.

2.3 Feasibility Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential. Three key considerations involved in the feasibility analysis are

2.3.1 Economical Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

2.3.2 Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

2.3.3 Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

2.4 System Requirement Specification

2.4.1 Functional Requirements

The Functional Requirements Document (FRD) is a formal statement of an application's functional requirements. It serves the same purpose as a contract. Here, the developers agree to provide the capabilities specified. The client agrees to find the product satisfactory if it provides the capabilities specified in the FRD.

Functional requirements capture the intended behavior of the system. This behavior may be expressed as services, tasks or functions the system is required to perform. The document should be tailored to fit a particular project's need. They define things such as system calculations, data manipulation and processing, user interface and interaction with the application.

The Functional Requirements Document (FRD) has the following characteristics −

- It demonstrates that the application provides value in terms of the business objectives and business processes in the next few years.
- It contains a complete set of requirements for the application. It leaves no room for anyone to assume anything which is not stated in the FRD.
- It is solution independent. The ERD is a statement of what the application is to do— not of how it works. The FRD does not commit the developers to a design. For that reason, any reference to the use of a specific technology is entirely inappropriate in an FRD.

The functional requirement should include the following −

- Descriptions of data to be entered into the system
- Descriptions of operations performed by each screen
- Descriptions of work-flows performed by the system
- Descriptions of system reports or other outputs
- Who can enter the data into the system?

- How the system meets applicable regulatory requirements?

The functional specification is designed to be read by a general audience. Readers should understand the system, but no technical knowledge should be required to understand this document.

Functional Requirements Deliverables

A Business Requirements Document (BRD) consists of −

- **Functional Requirements** − A document containing detailed requirements for the system being developed. These requirements define the functional features and capabilities that a system must possess. Be sure that any assumptions and constraints identified during the Business Case are still accurate and up to date.
- **Business Process Model** − A model of the current state of the process ("as is" model) or a concept of what the process should become ("to be" model)
- **System Context Diagram** − A Context Diagram shows the system boundaries, external and internal entities that interact with the system, and the relevant data flows between these external and internal entities.
- **Flow Diagrams (as-is or to-be)** − Diagrams graphically depict the sequence of operations or the movement of data for a business process. One or more flow diagrams are included depending on the complexity of the model.
- **Business Rules and Data Requirements** − Business rules define or constrain some aspects of the business and are used to define data constraints, default values, value ranges, cardinality, data types, calculations, exceptions, required elements and the relational integrity of the data.
- **Data Models** − Entity Relationship Diagrams, Entity Descriptions, Class Diagrams
- **Conceptual Model** − High level display of different entities for a business function and how they relate to one another.
- **Logical Model** − Illustrates the specific entities, attributes and relationships involved in a business function and represents all the definitions, characteristics, and relationships of data in a business, technical, or conceptual environment.
- **Data Dictionary and Glossary** − A collection of detailed information on the data elements, fields, tables and other entities that comprise the data model underlying a database or similar data management system.
- **Stakeholder Map** − Identifies all stakeholders who are affected by the proposed change and their influence/authority level for requirements. This document is developed in the origination phase of the Project Management Methodology (PMM) and is owned by the Project Manager but to be updated by the project team as new/changed Stakeholders are identified throughout the process.

- **Requirements Traceability Matrix** – A table that illustrates logical links between individual functional requirements and other types of system artifacts, including other Functional Requirements, Use-cases/User Stories, Architecture and Design Elements, Code Modules, Test Cases, and Business Rules

2.4.2 Non Functional Requirements

Non-functional requirements define the overall qualities or attributes of the resulting System Non-functional requirements place restrictions on the product being developed, the development process, and specify external constraints that the product must meet. Examples of NFR include safety, security, usability, reliability and performance Requirements. Project management issues (costs, time, and schedule) are often considered as non-functional requirements.

Performance requirements

Requirements about resources required, response time, transaction rates, throughput, benchmark specifications or anything else having to do with performance. In this project, Data publisher (or data holder, who collects data from record owner ex. Alice and bob) and data miner or the public, called the data recipient and record owners like patients and doctors.

Modifiability

Requirements about the effort required to make changes in the software. Often, the measurement is personnel effort (person- months).

Portability

The effort required to move the software to a different target platform. The measurement is most commonly person-months or % of modules that need changing.

Reliability

Requirements about how often the software fails. The measurement is often expressed in MTBF (mean time between failures). The definition of a failure must be clear. Also, don't confuse reliability with availability which is quite a different kind of requirement. Be sure to specify the consequences of software failure, how to protect from failure, a strategy for error detection, and a strategy for correction.

Security

One or more requirements about protection of your system and its data. The measurement can be expressed in a variety of ways (effort, skill level, time) to break into the system. Do not discuss solutions (e.g. passwords) in a requirements document.

Usability

Requirements about how difficult it will be to learn and operate the system. The requirements are often expressed in learning time or similar metrics.

Legal

There may be legal issues involving privacy of information, intellectual property rights, export of restricted technologies, etc.

2.5 Hardware Requirements

• System	:	Pentium IV 2.4 GHz.
• Hard Disk	:	40 GB.
• RAM	:	512 Mb.

2.6 Software Requirements

• Operating system	:	Windows 7 Ultimate.
• Coding Language	:	Python.
• Front-End	:	Python with Django.
• Designing	:	Html, CSS, JavaScript.
• Data Base	:	MySQL.

3. SYSTEM DESIGN

3.1 System Architecture

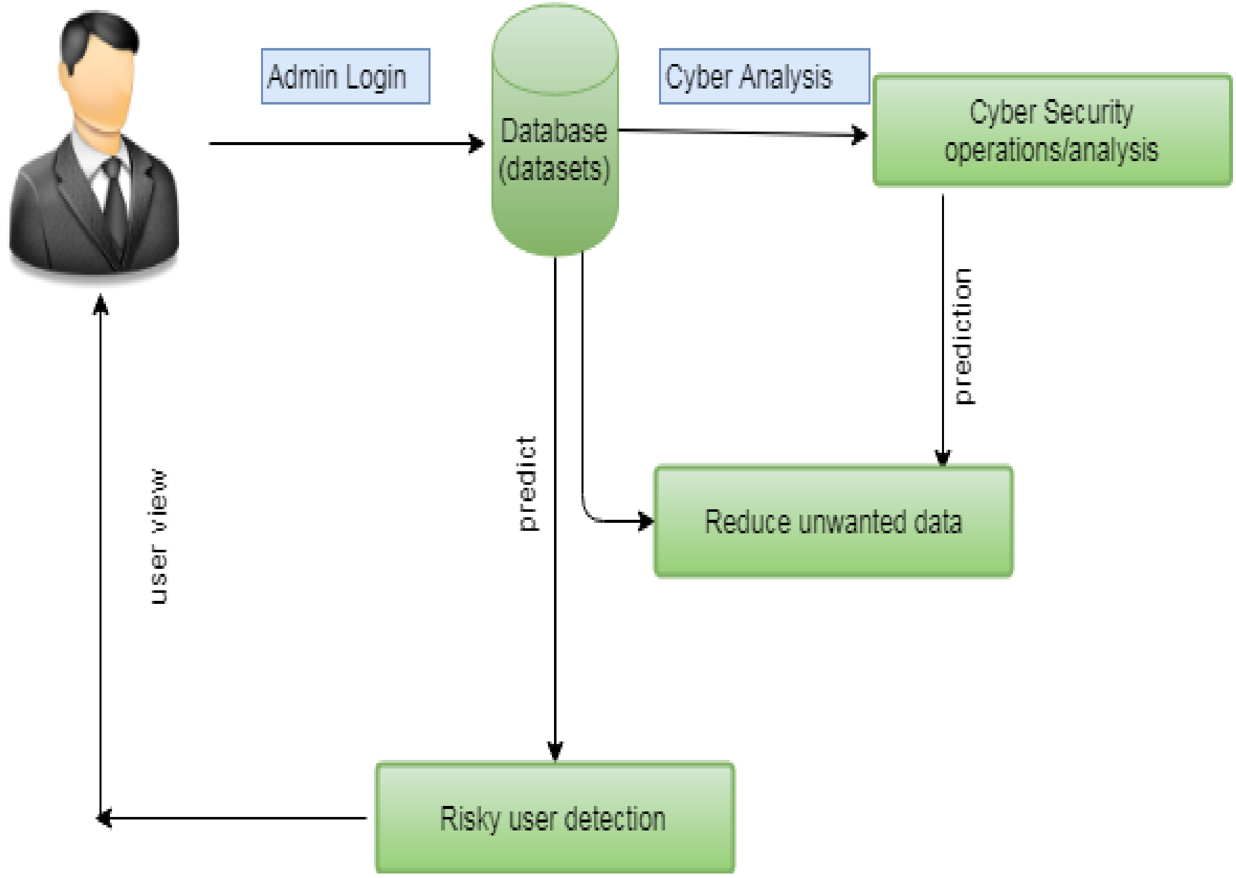


Fig:3.1 System Architecture

3.2 Modules

Cyber Analysis

Cyber threat analysis is a process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber-attacks. With respect to cyber security, this threat-oriented approach to combating cyber-attacks represents a smooth transition from a state of reactive security to a state of proactive one. Moreover, the desired result of a threat assessment is to give best practices on how to maximize the protective instruments with respect to availability, confidentiality and integrity, without turning back to usability and functionality conditions. CYPER ANALYSIS a threat could be anything that leads to interruption, meddling or destruction of any valuable service or item existing in the firm's repertoire. Whether of "human" or "nonhuman" origin, the analysis must scrutinize each element that may bring about conceivable security risk.

Dataset Modification

If a dataset in your dashboard contains many dataset objects, you can hide specific dataset objects from display in the Datasets panel. For example, if you decide to import a large amount of data from a file, but do not remove every unwanted data column before importing the data into Web, you can hide the unwanted attributes and metrics, To hide dataset objects in the Datasets panel, To show hidden objects in the Datasets panel, To rename a dataset object, To create a metric based on an attribute, To create an attribute based on a metric, To define the geo role for an attribute, To create an attribute with additional time information, To replace a dataset object in the dashboard.

Data Reduction

Improve storage efficiency through data reduction techniques and capacity optimization using data reduplication, compression, snapshots and thin provisioning. Data reduction via simply deleting unwanted or unneeded data is the most effective way to reduce a storing's data

Risky User Detection

False alarm immunity to prevent customer embarrassment, High detection rate to protect all kinds of goods from theft, Wide-exit coverage offers greater flexibility for entrance/exit layouts, Wide range of attractive designs complement any store décor, Sophisticated digital controller technology for optimum system performance

Algorithm

Support Vector Machine(SVM)

"Support Vector Machine" (SVM) is a supervised machine learning algorithm which can be used for both classification or regression challenges. However, it is mostly used in classification problems. In this algorithm, we plot each data item as a point in n-dimensional space (where n is number of features you have) with the value of each feature being the value of a particular coordinate. Then, we perform classification by finding the hyper-plane that differentiate the two classes very well (look at the below snapshot). The SVM algorithm is implemented in practice using a kernel. The learning of the hyperplane in linear SVM is done by transforming the problem using some linear algebra, which is out of the scope of this introduction to SVM. A powerful insight is that the linear SVM can be rephrased using the inner product of any two given observations, rather than the observations themselves. The inner product between two vectors is the sum of the multiplication of each pair of input values. For example, the inner product of the vectors [2, 3] and [5, 6] is 2*5 + 3*6 or 28. The equation for making a prediction for a new input using the dot product between the input (x) and each support vector (xi) is calculated as follows:

f(x) = B0 + sum(ai * (x,xi))

This is an equation that involves calculating the inner products of a new input vector (x) with all support vectors in training data. The coefficients B0 and ai (for each input) must be estimated from the training data by the learning algorithm.

3.3 UML Diagrams

The underlying premise of UML is that no one diagram can capture the different elements of a System in its entirety. Hence, UML is made up of nine diagrams that can be used to model a System at different points of time in the software life cycle of a system.

A software system can be said to have two distinct characteristics: a structural, "static" part and a behavioral, "dynamic" part. In addition to these two characteristics, an additional characteristic that a software system possesses is related to implementation. Before we categorize UML diagrams into each of these three characteristics, let us take a quick look at exactly what these characteristics are.

- Use case diagram
- Class diagram
- Object diagram
- State diagram
- Activity diagram
- Sequence diagram
- Collaboration diagram
- Component diagram
- Deployment diagram

3.3.1 Use Case Diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

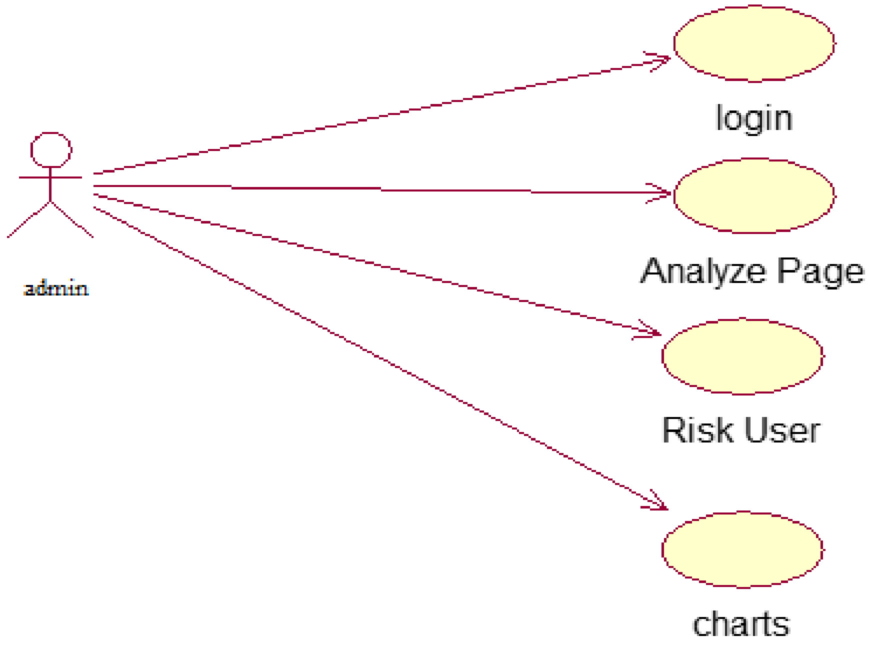


Fig:3.2 Use Case Diagram For Admin

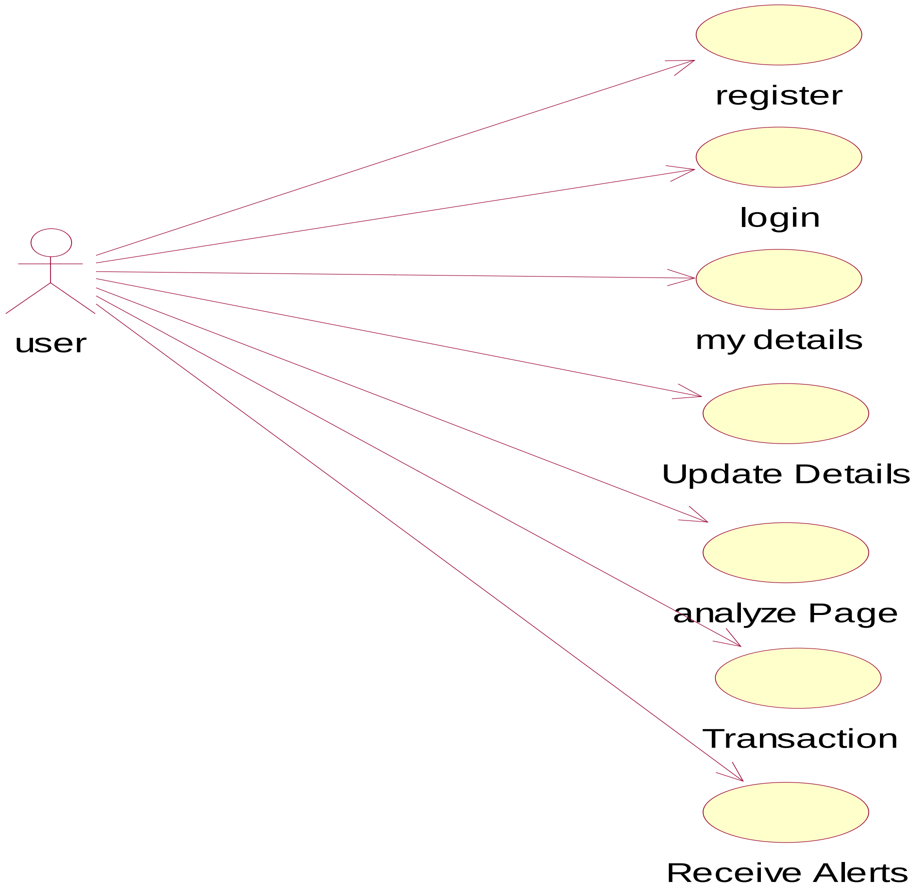


Fig:3.3 Use Case Diagram For User

3.3.2 Class Diagram:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

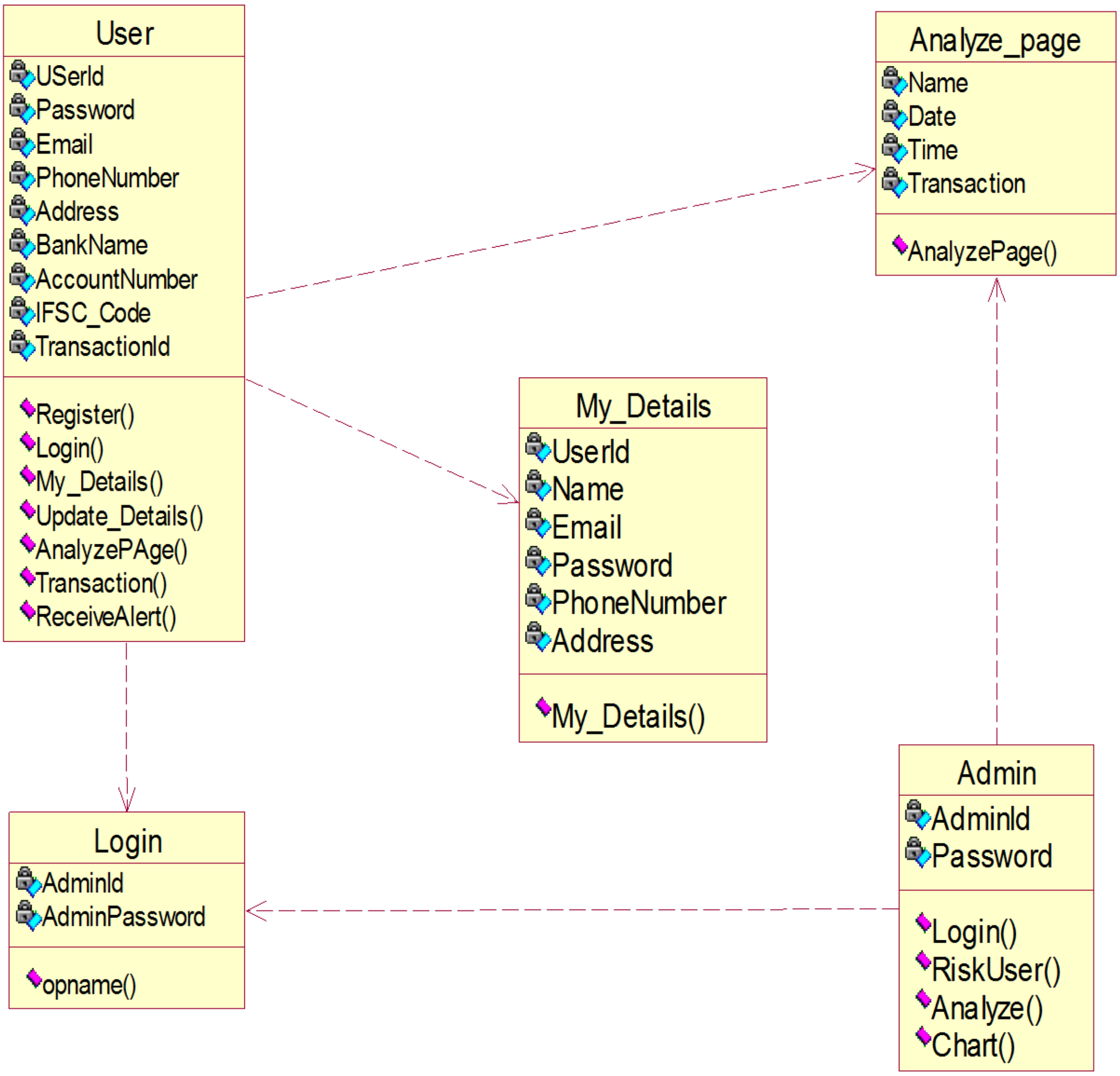


Fig:3.4 Class Diagram

3.3.3 Sequential Diagram

A sequence diagram represents the interaction between different objects in the system. The Important aspect of a sequence diagram is that it is time-ordered. Different objects In the sequence diagram interact with each other by passing "messages".

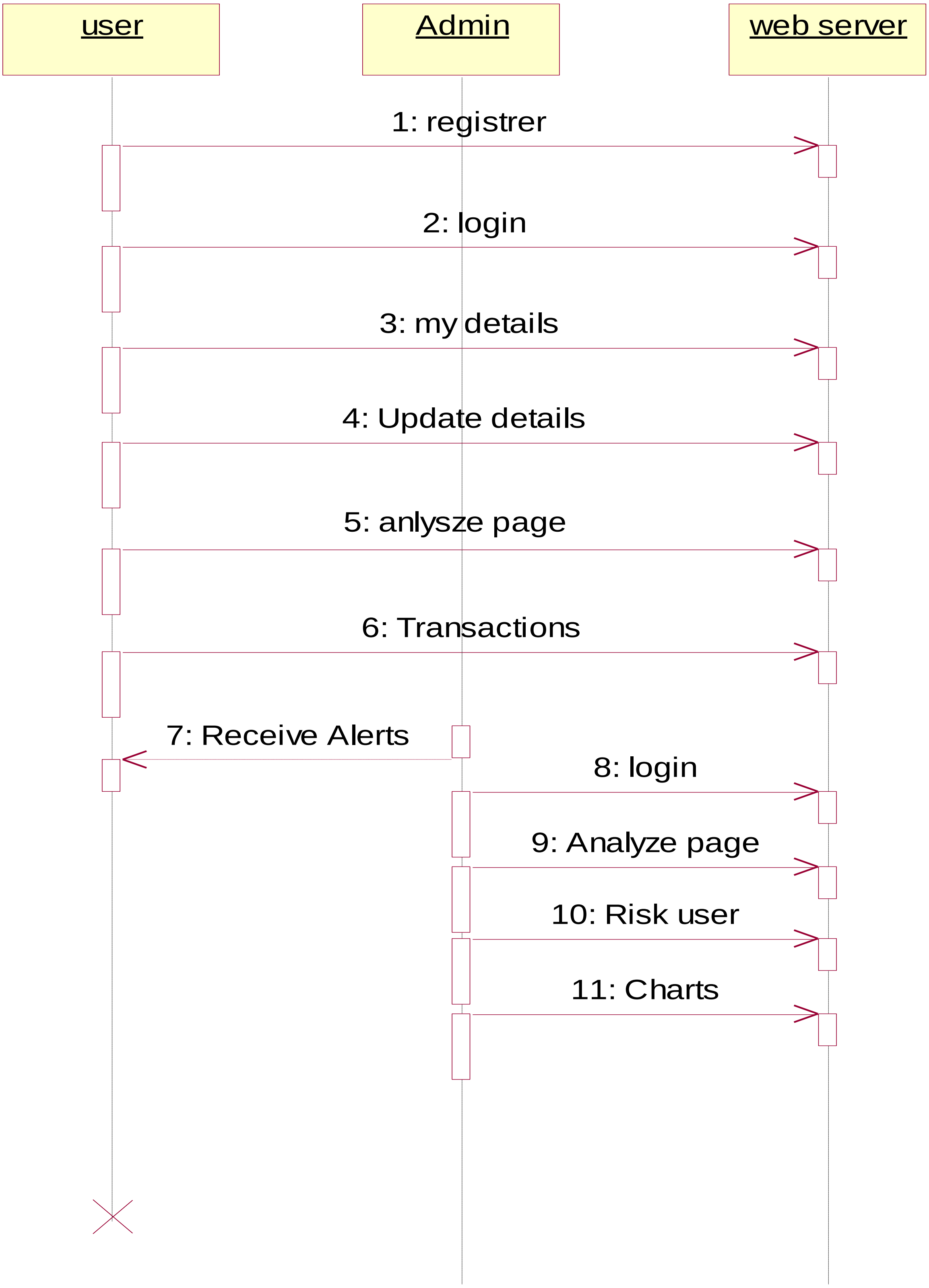


Fig:3.5 Sequential Diagram

3.3.4 Component Diagram

The process of this diagram shows the organizations and dependencies among a set of components.it represents the static implementation view of a system.

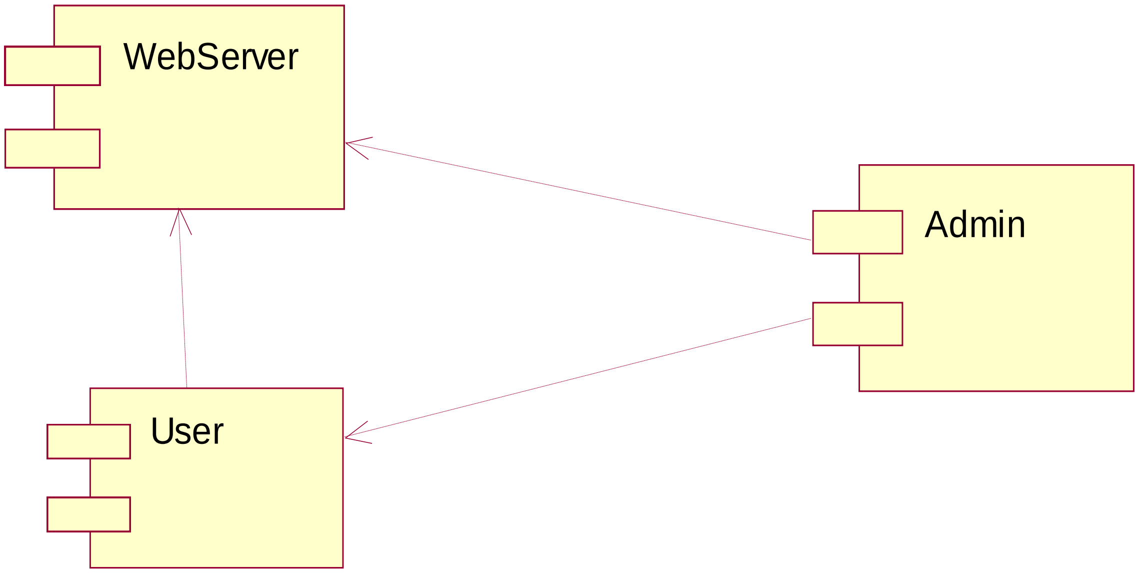


Fig:3.6 Component Diagram

3.3.5 Deployment Diagram

The deployment diagram captures the configuration of the runtime elements of the Application. This diagram is by far most useful when a system is built and ready to be Deployed.

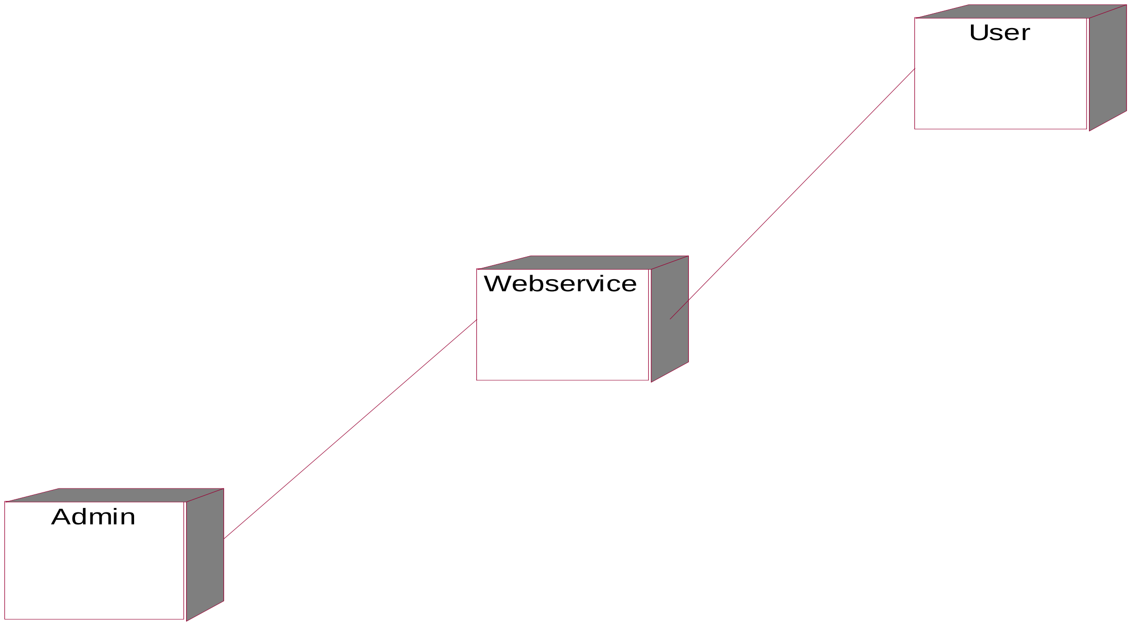


Fig:3.7 Deployment Diagram

3.4 Database Design

The data pertaining to proposed system is voluminous that a careful design of the database must proceed before storing the data in the database. A database management system Provides flexibility in the storage and retrieval of data bad production of information. The DBMS is a bridge between the application programs, which determines what data are Needed and how they are processed, and the operating system of the computer, which is Responsible for placing data on the magnetic storage devices. A schema defines the Database and a subschema defines the portion of the database that a specific program will Use.

3.4.1 Normalization

Normalization theory is built around the concept of normal forms. A relation is said to be in particular normal form if it satisfies a certain specified set of constraints.

First Normal form

A relation R is in first normal form if and only if all underlying domains contained atomic values only

Second Normal form

A relation R is said to be in second normal form if and only if it is in first normal form and every non-key attribute is fully dependent on the primary key.

Third Normal form

A relation R is said to be in third normal form if and only if it is in second normal form and every non key attribute is non transitively depend on the primary key.

Boyce and Codd Normal Form (BCNF)

Boyce and Codd Normal Form is a higher version of the Third Normal form. This form deals with certain type of anomaly that is not handled by 3NF. A 3NF table which does not have multiple overlapping candidate keys is said to be in BCNF. For a table to be in BCNF, following conditions must be satisfied:

- R must be in 3rd Normal Form
- and, for each functional dependency (X → Y), X should be a super Key.

Fourth Normal Form (4NF)

Fourth Normal Form comes into picture when Multi-valued Dependency occur in any relation. For a table to satisfy the Fourth Normal Form, it should satisfy the following two conditions:

1. It should be in the Boyce-Codd Normal Form.
2. zAnd, zthe table should not have any Multi-valued Dependency.

3.4.2 ER Diagram

a. User

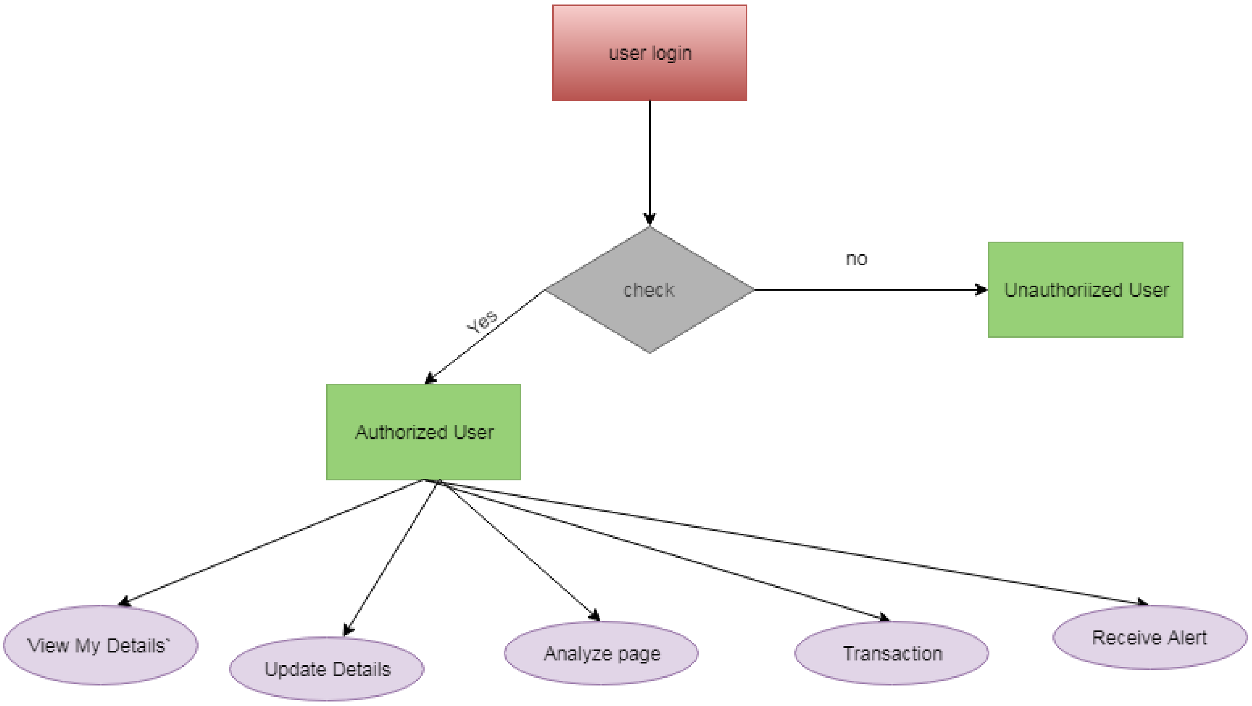


Fig:3.8 ER Diagram For User

b. admin

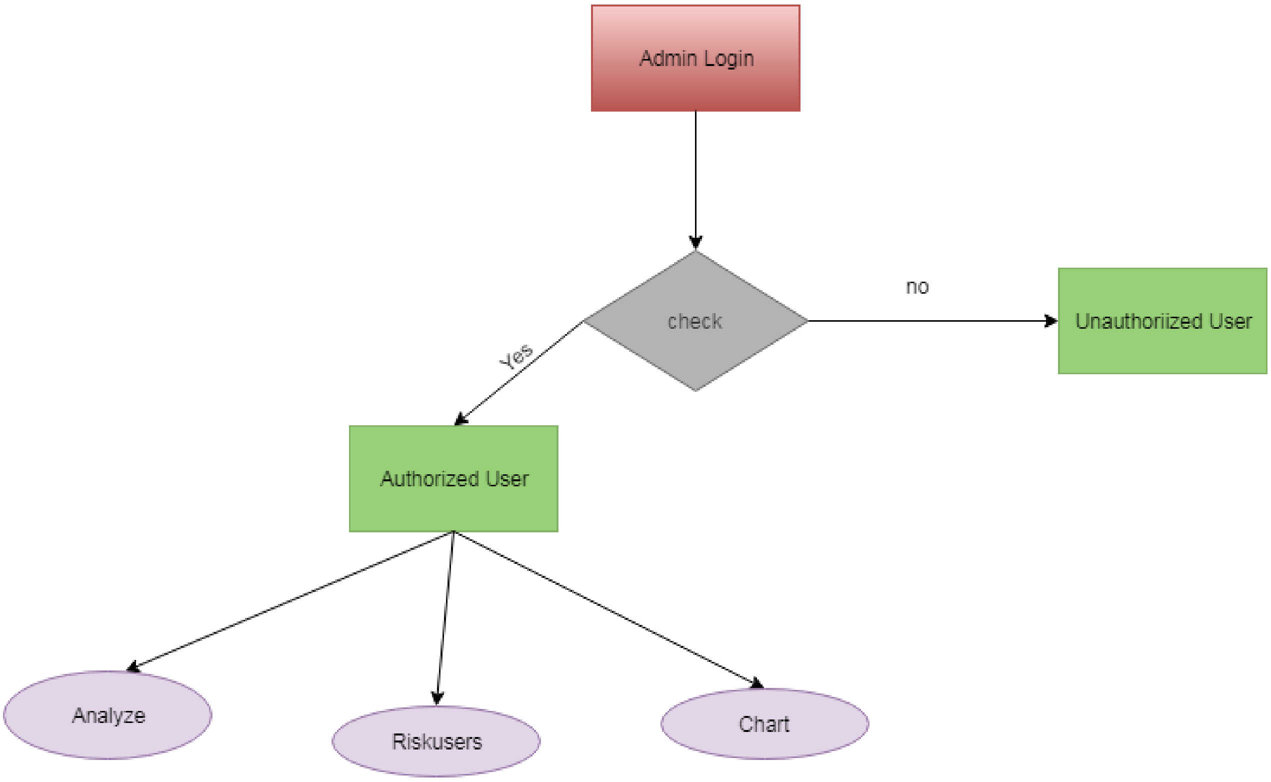


Fig:3.9 ER Diagram For Admin

4. SYSTEM IMPLEMENTATION

4.1 Front End Implementation

Python Introduction

Python is a general purpose, dynamic, high level, and interpreted programming language. 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 is easy to learn 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. It supports multiple programming pattern, including object-oriented, imperative, and functional or procedural programming styles.

Python is not intended to work in a particular area, such as web programming. That is why it is known as multipurpose programming language because it can be used with web, enterprise, 3D CAD, etc. We don't need to use data types to declare variable because it is dynamically typed so we can write a=10 to assign an integer value in an integer variable. It makes the development and debugging fast because there is no compilation step included in Python development, and edit-test-debug cycle is very fast.

Python Applications

Python is known for its general purpose nature that makes it applicable in almost each domain of software development. Python as a whole can be used in any sphere of development. Here, we are specifying applications areas where python can be applied.

- **Web Applications:** We can use Python to develop web applications. It provides libraries to handle internet protocols such as HTML and XML, JSON, Email processing, request, beautiful Soup, Feed parser etc. It also provides Frameworks such as Django, Pyramid, Flask etc to design and develop web based applications. Some important developments are: PythonWikiEngines, Pocoo, PythonBlogSoftware etc.
- **Desktop GUI Applications:** Python provides Tk GUI library to develop user interface in python based application. Some other useful toolkits wxWidgets, Kivy, pyqt that are useable on several platforms. The Kivy is popular for writing multitouch applications.
- **Software Development:** Python is helpful for software development process. It works as a support language and can be used for build control and management, testing etc.

- **Scientific and Numeric:** Python is popular and widely used in scientific and numeric computing. Some useful library and package are SciPy, Pandas, IPython etc. SciPy is group of packages of engineering, science and mathematics.
- **Business Application:** Python is used to build Business applications like ERP and e-commerce systems. Tryton is a high level application platform.
- **Console Based Application:** We can use Python to develop console based applications. For example: IPython.
- **Audio or Video based Applications:** Python is awesome to perform multiple tasks and can be used to develop multimedia applications. Some of real applications are: TimPlayer, cplay etc.\
- **3D CAD Applications:** To create CAD application Fandango is a real application which provides full features of CAD.
- **Enterprise Applications:** Python can be used to create applications which can be used within an Enterprise or an Organization. Some real time applications are: OpenErp, Tryton, Picalo etc.
- **Applications for Images:** Using Python several application can be developed for image. Applications developed are: VPython, Gogh, imgSeek etc.

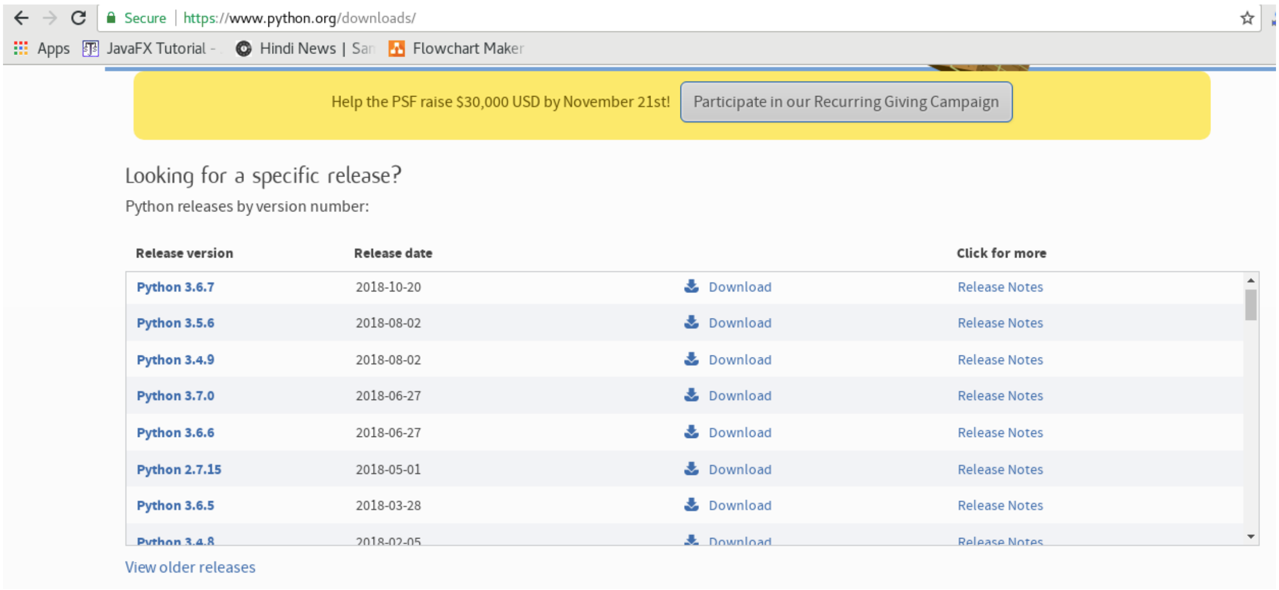
There are several such applications which can be developed using Python

How to Install Python (Environment Set-up)

In this section of the tutorial, we will discuss the installation of python on various operating systems.

Installation on Windows:

Visit the link *https://www.python.org/downloads/* to download the latest release of Python. In this process, we will install Python 3.6.7 on our Windows operating system.



Secure
https://www.python.org/downloads/
Apps
JavaFX Tutorial -
Hindi News | Sar
Flowchart Maker
Participate in our Recurring Giving Campaign
View older releases

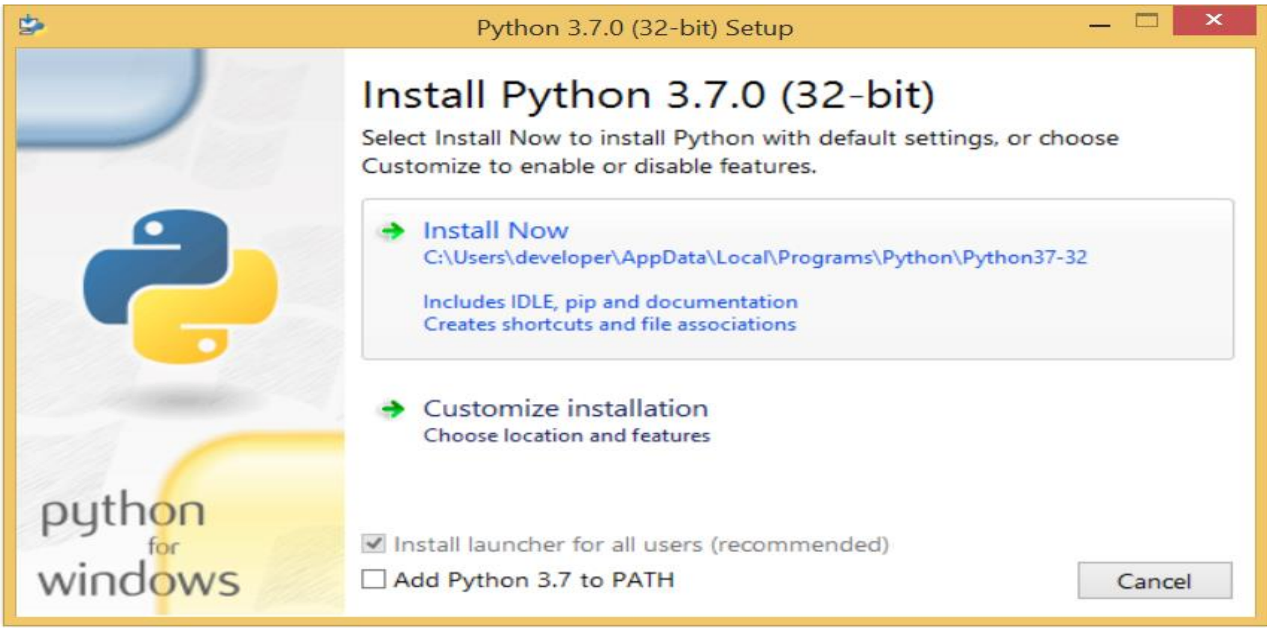
Help the PSF raise $30,000 USD by November 21st!

Looking for a specific release?

Python releases by version number:

Release version	Release date		Click for more
Python 3.6.7	2018-10-20	Download	Release Notes
Python 3.5.6	2018-08-02	Download	Release Notes
Python 3.4.9	2018-08-02	Download	Release Notes
Python 3.7.0	2018-06-27	Download	Release Notes
Python 3.6.6	2018-06-27	Download	Release Notes
Python 2.7.15	2018-05-01	Download	Release Notes
Python 3.6.5	2018-03-28	Download	Release Notes
Python 3.4.8	2018-02-05	Download	Release Notes

Double-click the executable file which is downloaded; the following window will open. Select Customize installation and proceed.



Python 3.7.0 (32-bit) Setup

Install Python 3.7.0 (32-bit)

Select Install Now to install Python with default settings, or choose Customize to enable or disable features.

→ Install Now
C:\Users\developer\AppData\Local\Programs\Python\Python37-32

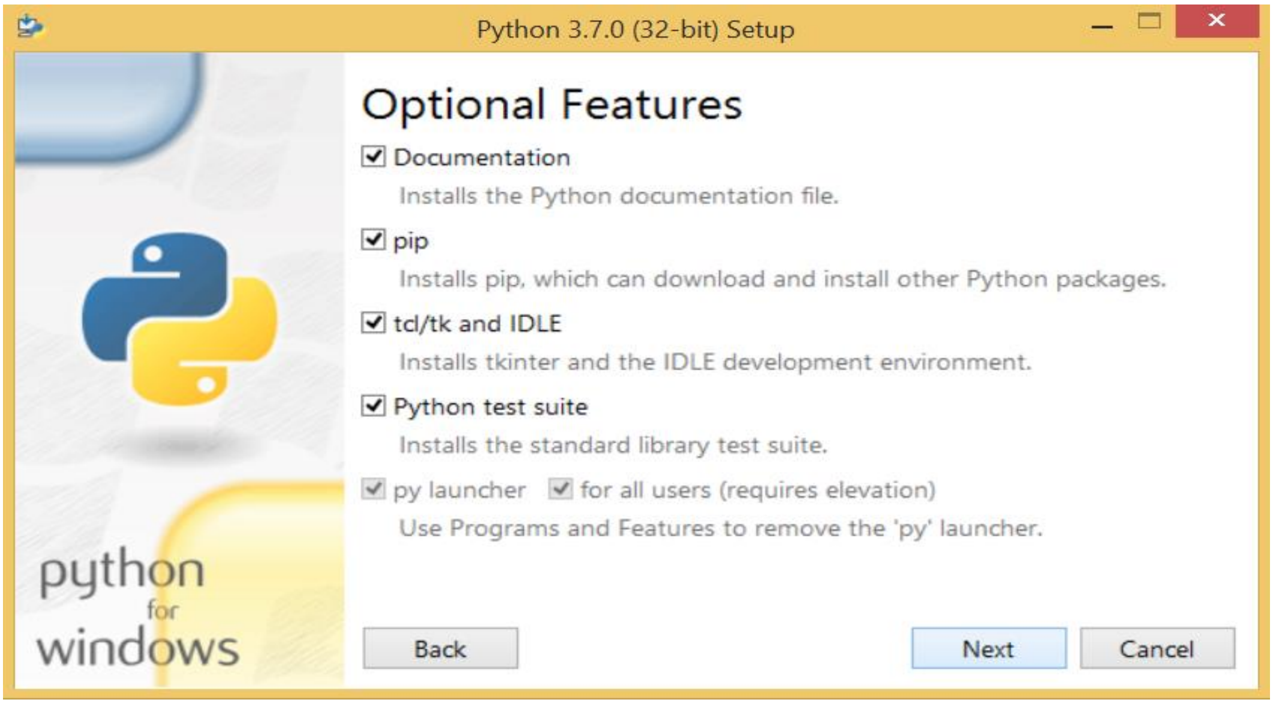
Includes IDLE, pip and documentation
Creates shortcuts and file associations

→ Customize installation
Choose location and features

☑ Install launcher for all users (recommended)
□ Add Python 3.7 to PATH

Fig:4.1 Python Installation

The following window shows all the optional features. All the features need to be installed and are checked by default; we need to click next to continue.



Python 3.7.0 (32-bit) Setup

Optional Features

☑ Documentation
Installs the Python documentation file.

☑ pip
Installs pip, which can download and install other Python packages.

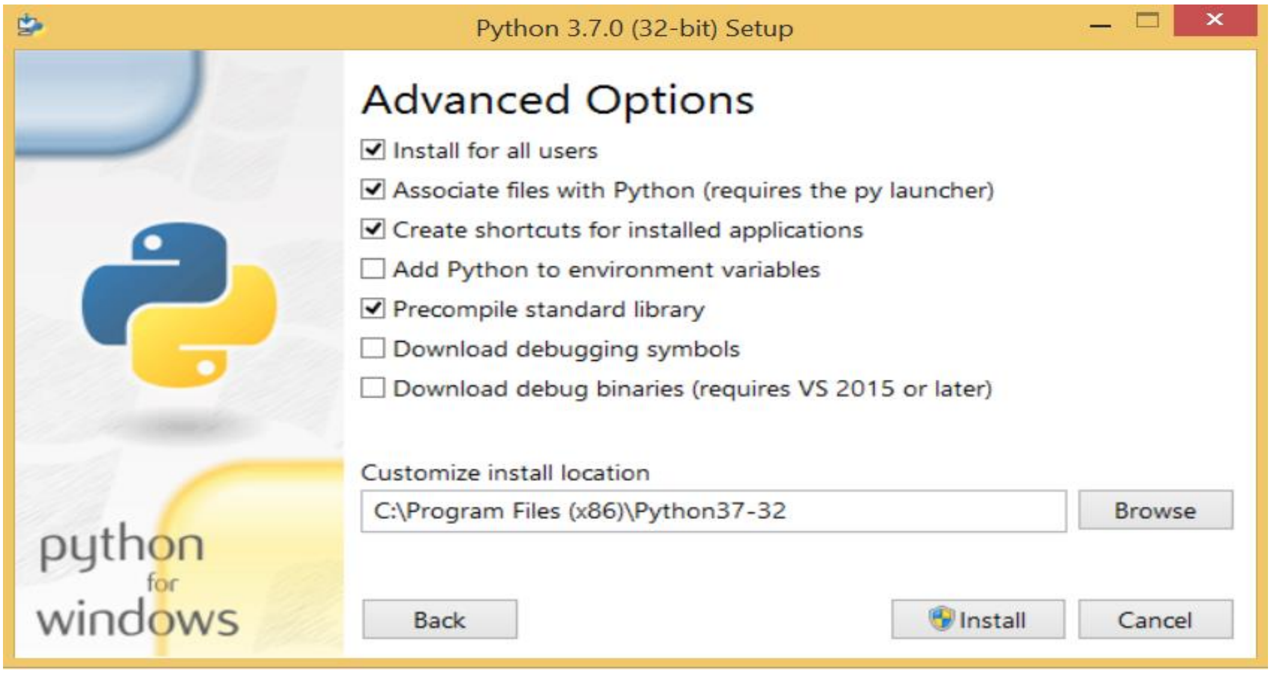
☑ tcl/tk and IDLE
Installs tkinter and the IDLE development environment.

☑ Python test suite
Installs the standard library test suite.

☑ py launcher ☑ for all users (requires elevation)
Use Programs and Features to remove the 'py' launcher.

Fig:4.2 Python Setup

The following window shows a list of advanced options. Check all the options which you want to install and click next. Here, we must notice that the first check-box (install for all users) must be checked.



Python 3.7.0 (32-bit) Setup

Advanced Options

☑ Install for all users

☑ Associate files with Python (requires the py launcher)

☑ Create shortcuts for installed applications

□ Add Python to environment variables

☑ Precompile standard library

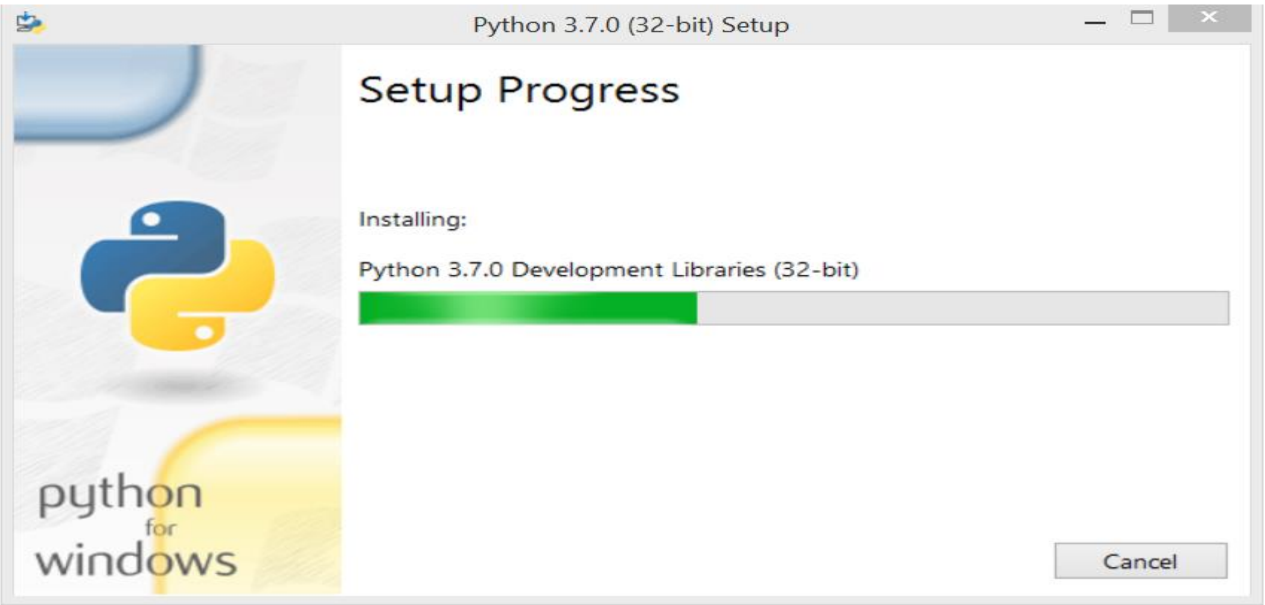
□ Download debugging symbols

□ Download debug binaries (requires VS 2015 or later)

Customize install location

C:\Program Files (x86)\Python37-32

Now, we are ready to install python-3.6.7. Let's install it.



Python 3.7.0 (32-bit) Setup

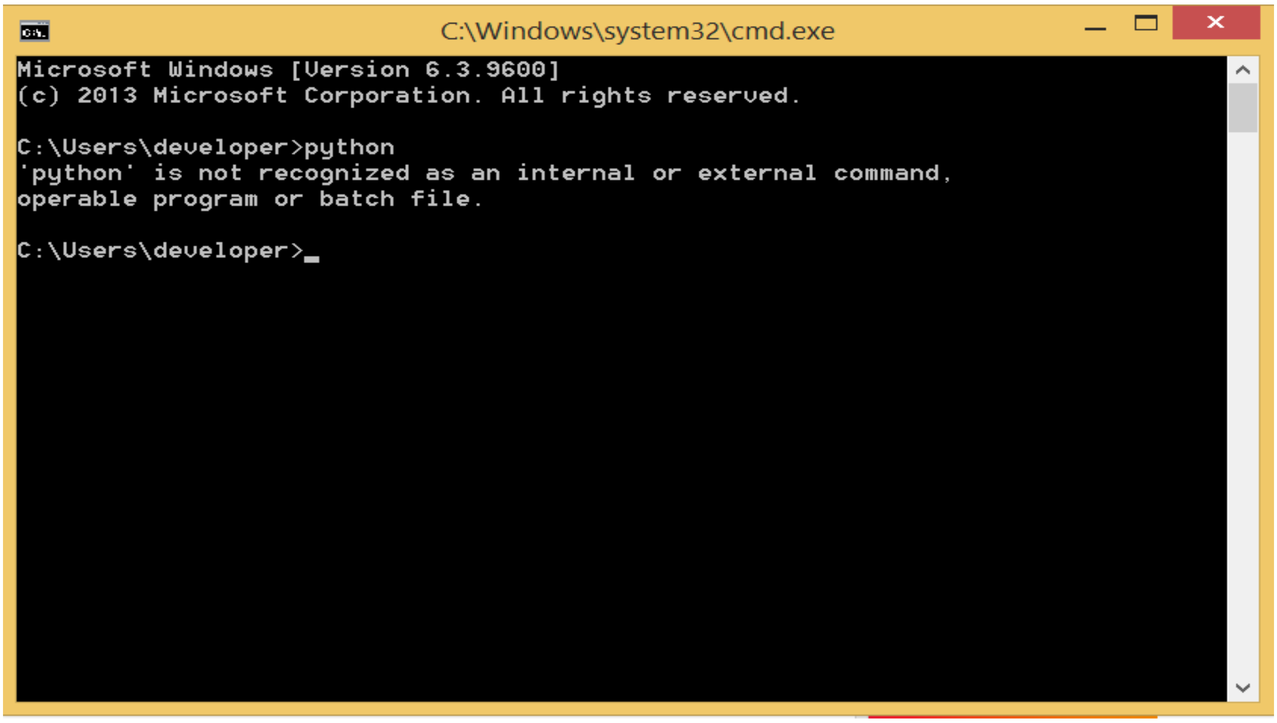
Setup Progress

Installing:

Python 3.7.0 Development Libraries (32-bit)

Fig:4.3 Python Setup Progress

Now, try to run python on the command prompt. Type the command **python** in case of python2 or python3 in case of **python3**. It will show an error as given in the below image. It is because we haven't set the path.

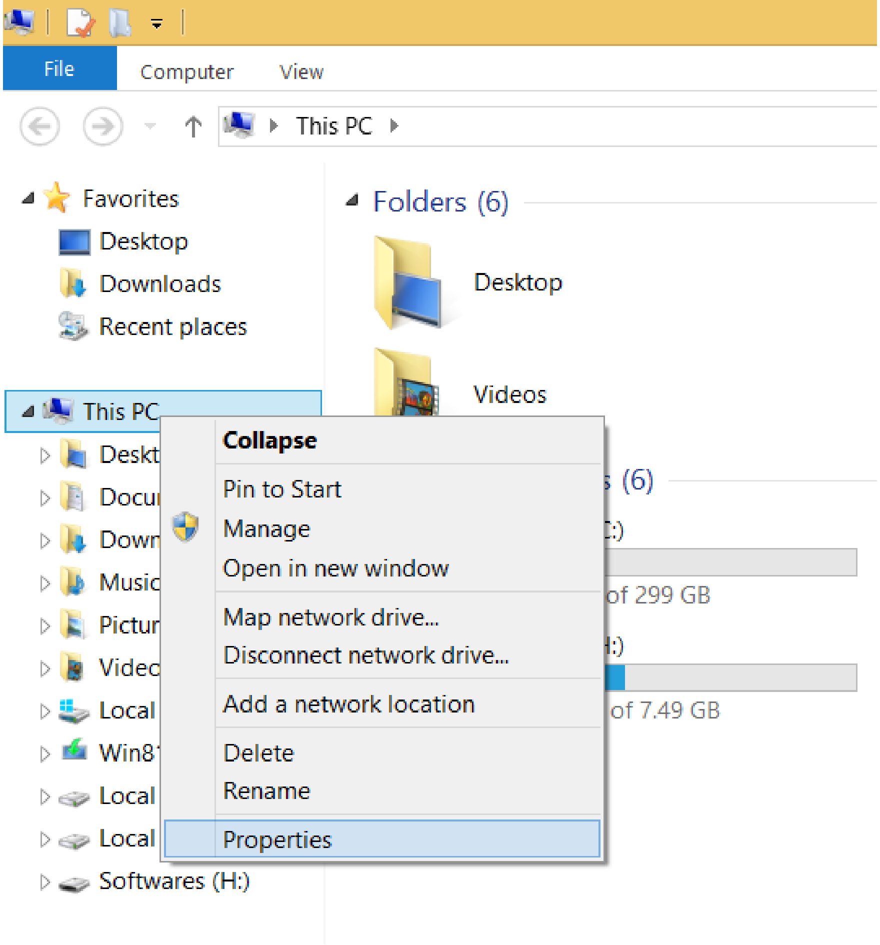


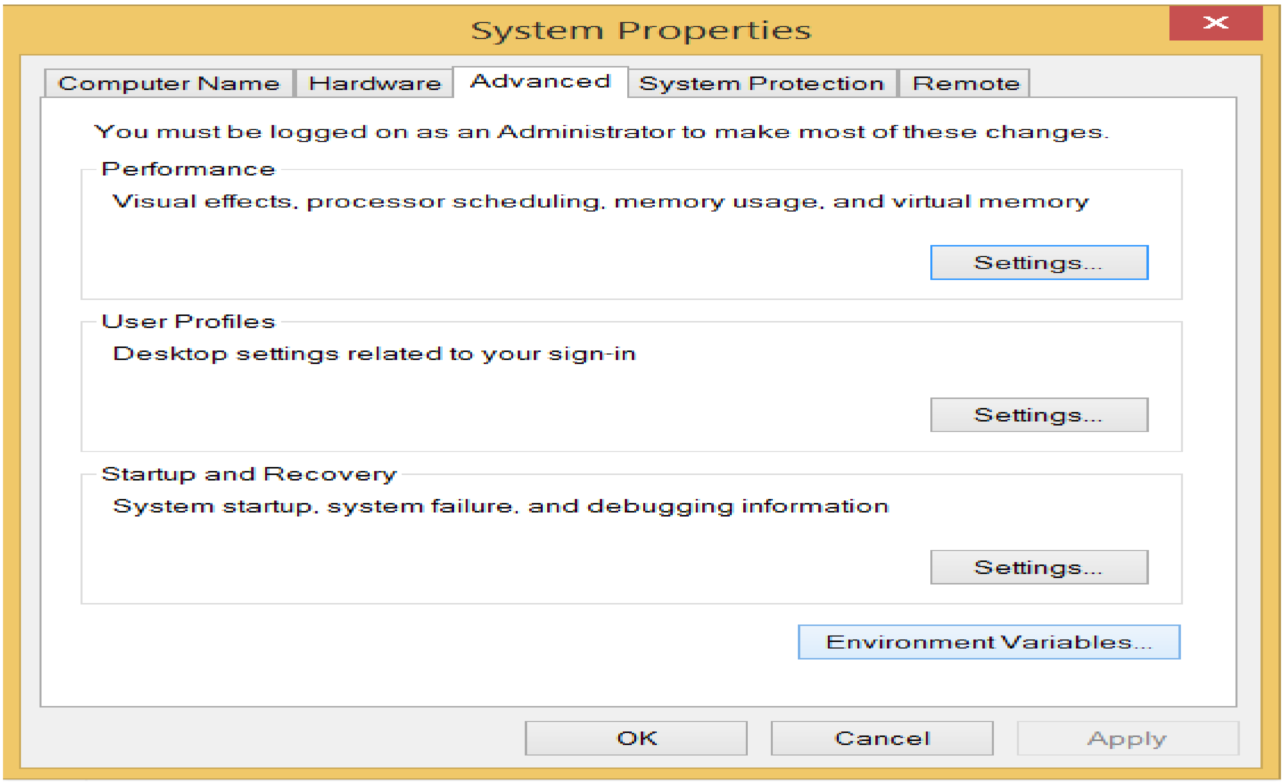
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\developer>python
'python' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\developer>_
```

To set the path of python, we need to the right click on "my computer" and go to Properties → Advanced → Environment Variables.





You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

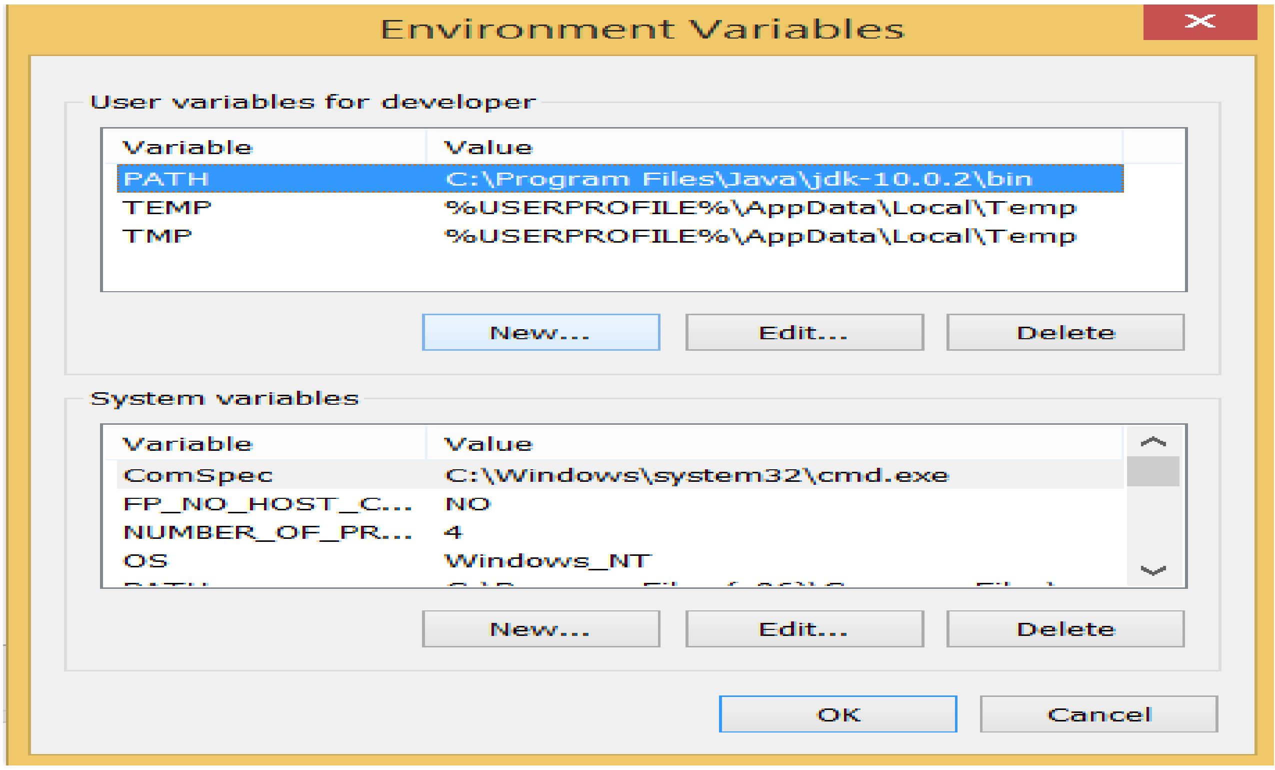
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

Add the new path variable in the user variable section.



User variables for developer

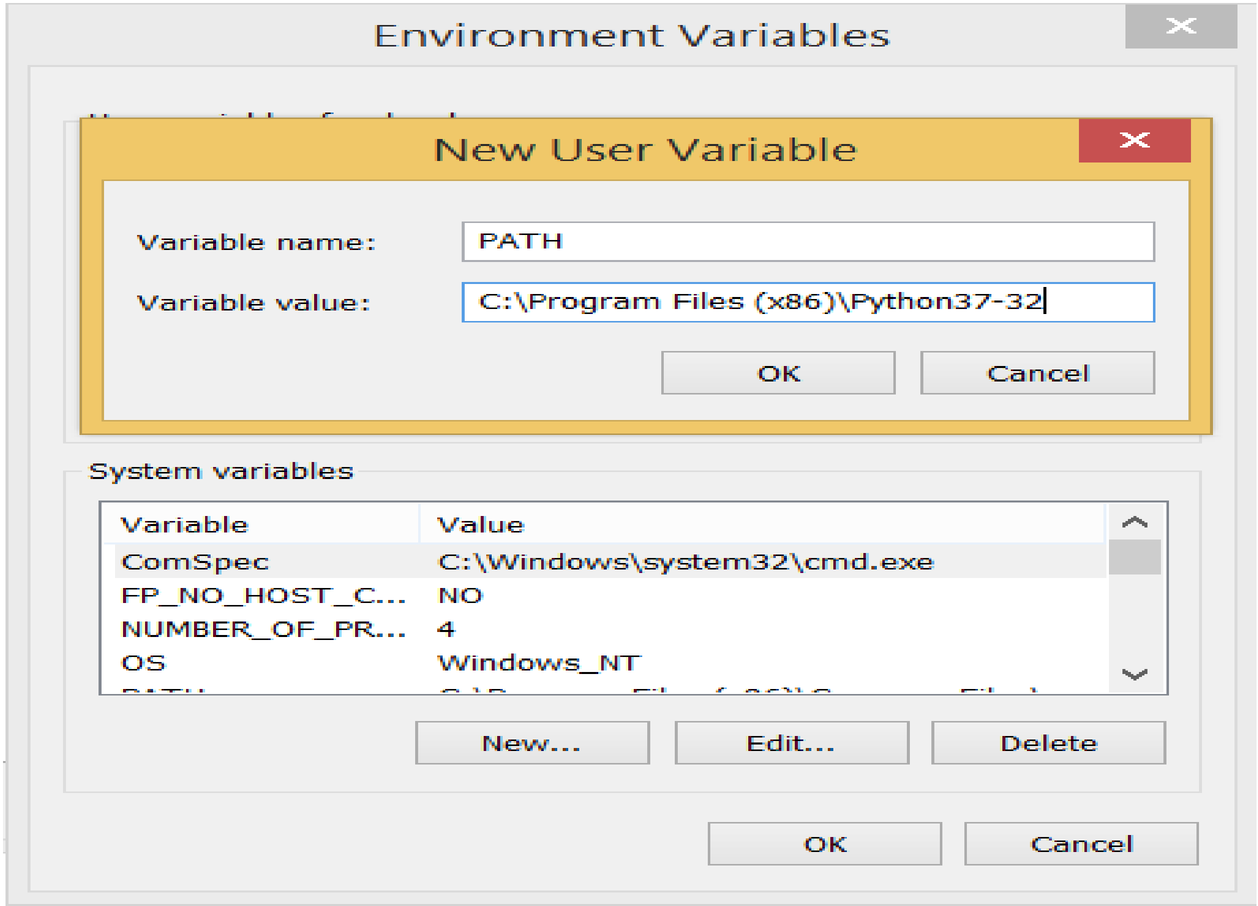
Variable	Value
PATH	C:\Program Files\Java\jdk-10.0.2\bin
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_C...	NO
NUMBER_OF_PR...	4
OS	Windows_NT

Fig:4.4 Python Path Setup

Type **PATH** as the variable name and set the path to the installation directory of the python shown in the below image.



Variable name: PATH

Variable value: C:\Program Files (x86)\Python37-32

System variables

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_C...	NO
NUMBER_OF_PR...	4
OS	Windows_NT

Now, the path is set, we are ready to run python on our local system. Restart CMD, and type **python** again. It will open the python interpreter shell where we can execute the python statements.

First Python Program

In this Section, we will discuss the basic syntax of python by using which, we will run a simple program to print hello world on the console.

Python provides us the two ways to run a program:

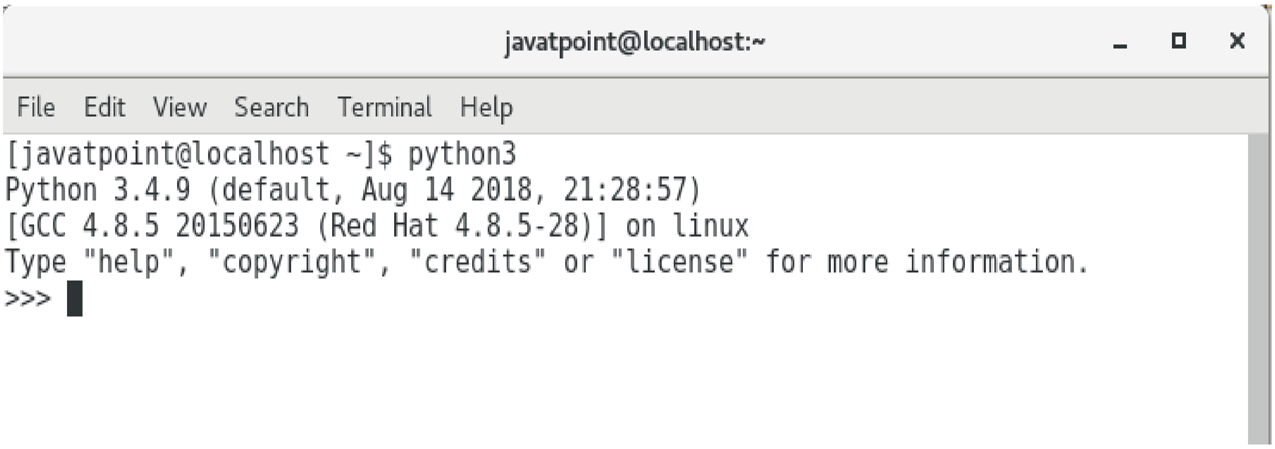
- Using Interactive interpreter prompt
- Using a script file

Let's discuss each one of them in detail.

Interactive interpreter prompt

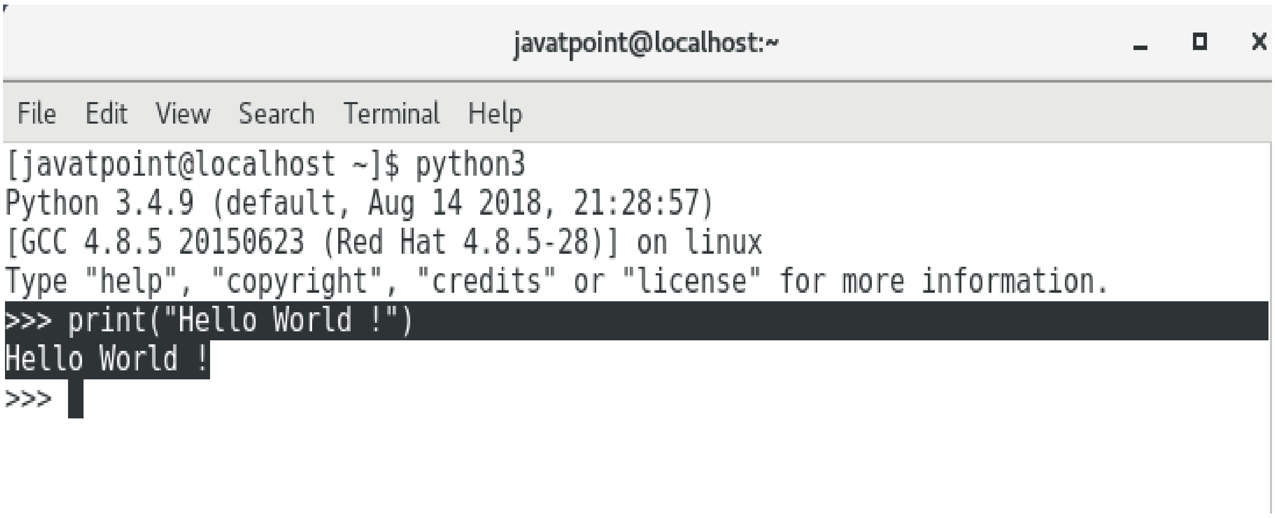
Python provides us the feature to execute the python statement one by one at the interactive prompt. It is preferable in the case where we are concerned about the output of each line of our python program. To open the interactive mode, open the terminal (or command prompt) and type python (python3 in case if you have python2 and python3 both installed on your system).

It will open the following prompt where we can execute the python statement and check their impact on the console.



```
[javatpoint@localhost ~]$ python3
Python 3.4.9 (default, Aug 14 2018, 21:28:57)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-28)] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 
```

Let's run a python statement to print the traditional hello world on the console. Python3 provides print() function to print some message on the console. We can pass the message as a string into this function. Consider the following image.



```
[javatpoint@localhost ~]$ python3
Python 3.4.9 (default, Aug 14 2018, 21:28:57)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-28)] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> print("Hello World !")
Hello World !
>>> 
```

Here, we get the message "Hello World !" printed on the console.

Using a script file

Interpreter prompt is good to run the individual statements of the code. However, we can not write the code every-time on the terminal. We need to write our code into a file which can be executed later. For this purpose, open an editor like notepad, create a file named first.py (python used .py extension) and write the following code in it.

- Print ("hello world"); #here, we have used print() function to print the message on the console. To run this file named as first.py, we need to run the following command on the terminal.

$ python3 first.py

Hence, we get our output as the message Hello World **!** is printed on the console.

Get Started with PyCharm

In our first program, we have used gedit on our CentOS as an editor. On Windows, we have an alternative like notepad or notepad++ to edit the code. However, these editors are not used as IDE for python since they are unable to show the syntax related suggestions. JetBrains provides the most popular and a widely used cross-platform IDE **PyCharm** to run the python programs.

PyCharm installation

As we have already stated, PyCharm is a cross-platform IDE, and hence it can be installed on a variety of the operating systems. In this section of the tutorial, we will cover the installation process of PyCharm on Windows, MacOS, CentOS, and Ubuntu.

Windows

Installing PyCharm on Windows is very simple. To install PyCharm on https://www.jetbrains.com/pycharm/download/download-thanks.html?platform=windows to download the executable installer. Double click the installer (.exe) file and install PyCharm by clicking next at each step.

DJANGO

Introduction

Django is a web application framework written in Python programming language. It is based on MVT (Model View Template) design pattern. The Django is very demanding due to its rapid development feature. It takes less time to build application after collecting client requirement. This framework uses a famous tag line: The web framework for perfectionists with deadlines**.** By using Django, we can build web applications in very less time. Django is designed in such a manner that it handles much of configure things automatically, so we can focus on application development only.

History

Django was design and developed by Lawrence journal world in 2003 and publicly released under BSD license in July 2005. Currently, DSF (Django Software Foundation) maintains its development and release cycle.

Django was released on 21, July 2005. Its current stable version is 2.0.3 which was released on 6 March, 2018.

Features of Django

- Rapid Development
- Secure
- Scalable
- Fully loaded
- Versatile
- Open Source
- Vast and Supported Community

Rapid Development

Django was designed with the intention to make a framework which takes less time to build web application. The project implementation phase is a very time taken but Django creates it rapidly.

- **Secure:** Django takes security seriously and helps developers to avoid many common security mistakes, such as SQL injection, cross-site scripting, cross-site request forgery etc. Its user authentication system provides a secure way to manage user accounts and passwords.
- **Scalable:** Django is scalable in nature and has ability to quickly and flexibly switch from small to large scale application project.
- **Fully loaded:** Django includes various helping task modules and libraries which can be used to handle common Web development tasks. Django takes care of user authentication, content administration, site maps, RSS feeds etc.
- **Versatile:** Django is versatile in nature which allows it to build applications for different-different domains. Now a days, Companies are using Django to build various types of applications like: content management systems, social networks sites or scientific computing platforms etc.
- **Open Source:** Django is an open source web application framework. It is publicly available without cost. It can be downloaded with source code from the public repository. Open source reduces the total cost of the application development.
- **Vast and Supported Community:** Django is an one of the most popular web framework. It has widely supportive community and channels to share and connect.

Django Installation

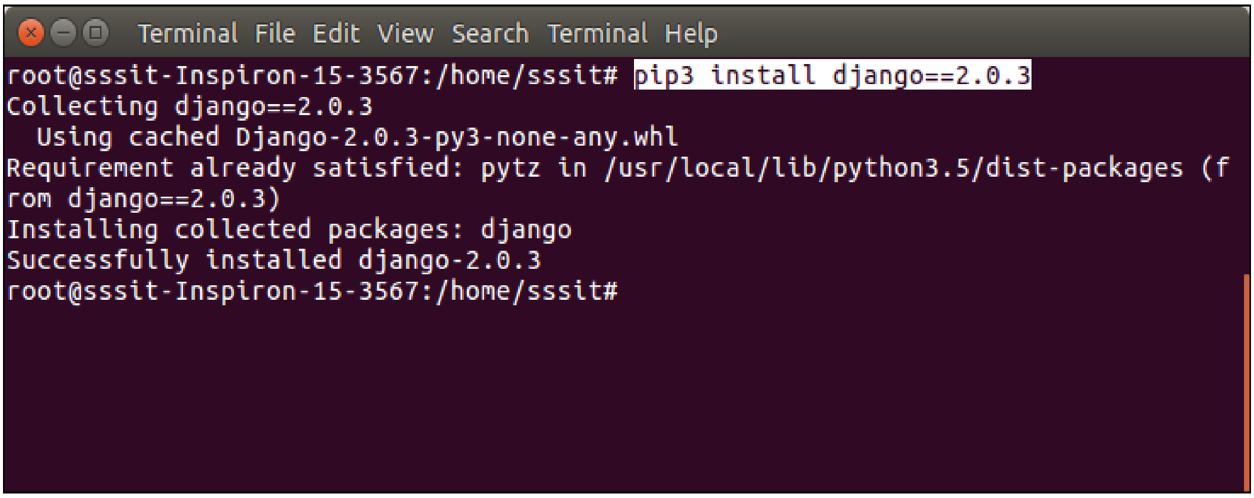
To install Django, first visit to django official site (https://www.djangoproject.com) and download django by clicking on the download section. Here, we will see various options to download The Django. Django requires pip to start installation. Pip is a package manager system which is used to install and manage packages written in python. For Python 3.4 and higher versions pip3 is used to manage packages.

In this tutorial, we are installing Django in Ubuntu operating system.

The complete installation process is described below. Before installing make sure pip is installed in local system.

Here, we are installing Django using pip3, the installation command is given below.

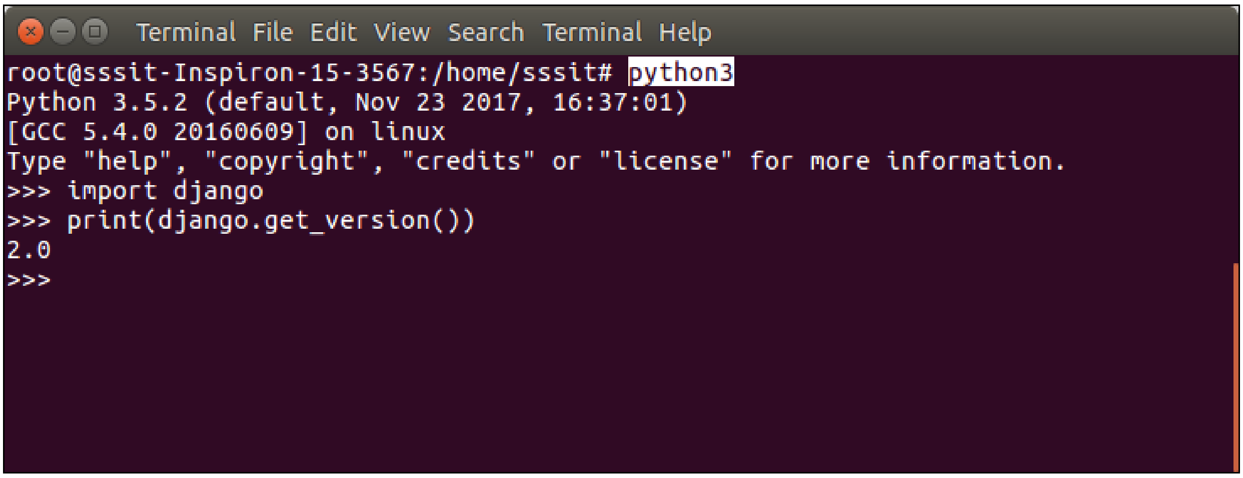
```
1. $ pip3 install django==2.0.3
```



```
root@sssit-Inspiron-15-3567:/home/sssit# pip3 install django==2.0.3
Collecting django==2.0.3
  Using cached Django-2.0.3-py3-none-any.whl
Requirement already satisfied: pytz in /usr/local/lib/python3.5/dist-packages (f
rom django==2.0.3)
Installing collected packages: django
Successfully installed django-2.0.3
root@sssit-Inspiron-15-3567:/home/sssit#
```

Verify Django Installation

After installing Django, we need to varify the installation. Open terminal and write **python3** and press enter. It will display python shell where we can verify django installation.



```
root@sssit-Inspiron-15-3567:/home/sssit# python3
Python 3.5.2 (default, Nov 23 2017, 16:37:01)
[GCC 5.4.0 20160609] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import django
>>> print(django.get_version())
2.0
>>>
```

Look at the Django version displayed by the print method of the python. Well, Django is installed successfully. Now, we can build Django web applications.

Django Project

In the previous topic, we have installed Django successfully. Now, we will learn step by step process to create a Django application.

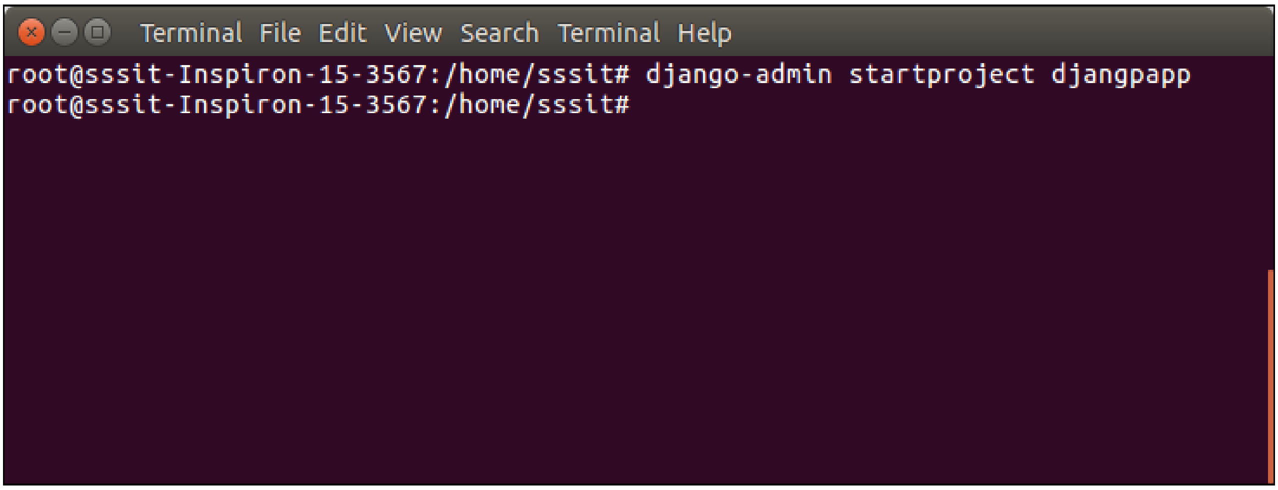
To create a Django project, we can use the following command. Project name is the name of Django application.

- $ django-admin start project project name

Django Project Example

Here, we are creating a project Djangpapp in the current directory.

- $ django-admin start project Djangpapp

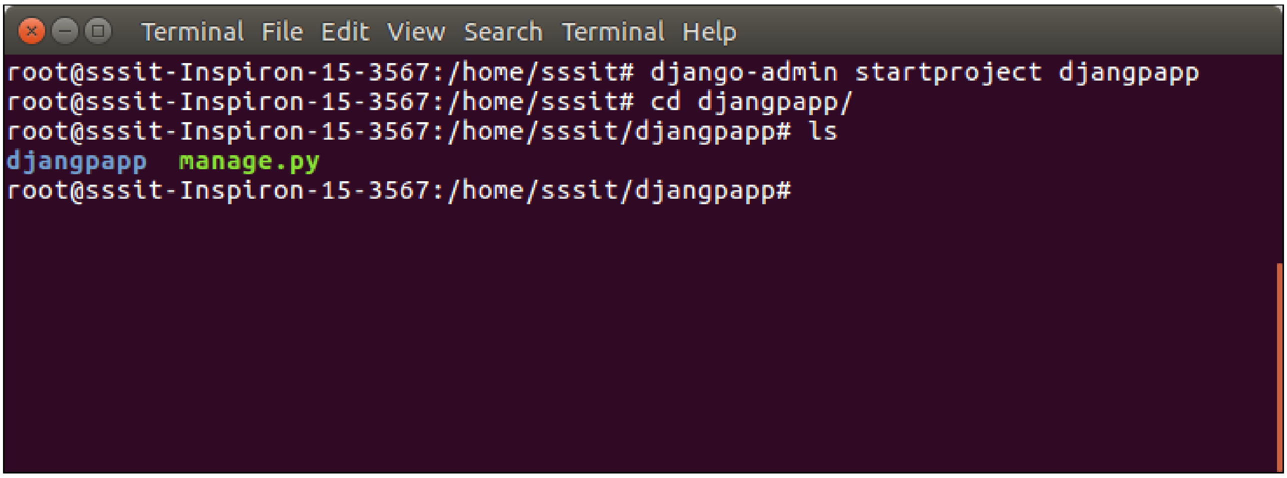


```
root@sssit-Inspiron-15-3567:/home/sssit# django-admin startproject djangpapp
root@sssit-Inspiron-15-3567:/home/sssit#
```

Locate into the Project

Now, move to the project by changing the directory. The Directory can be changed by using the following command.

- cd djangpapp



```
root@sssit-Inspiron-15-3567:/home/sssit# django-admin startproject djangpapp
root@sssit-Inspiron-15-3567:/home/sssit# cd djangpapp/
root@sssit-Inspiron-15-3567:/home/sssit/djangpapp# ls
djangpapp  manage.py
root@sssit-Inspiron-15-3567:/home/sssit/djangpapp#
```

To see all the files and subfolders of django project, we can use **tree** command to view the tree structure of the application. This is a utility command, if it is not present, can be downloaded via **apt-get install tree** command.

A Django project contains the following packages and files. The outer directory is just a container for the application. We can rename it further.

- **manage.py:** It is a command-line utility which allows us to interact with the project in various ways and also used to manage an application that we will see later on in this tutorial.
- **A directory** (djangpapp) located inside, is the actual application package name. Its name is the Python package name which we'll need to use to import module inside the application.
- **__init__.py:** It is an empty file that tells to the Python that this directory should be considered as a Python package.

- **settings.py:** This file is used to configure application settings such as database connection, static files linking etc.
- **urls.py:** This file contains the listed URLs of the application. In this file, we can mention the URLs and corresponding actions to perform the task and display the view.
- **wsgi.py:** It is an entry-point for WSGI-compatible web servers to serve Django project.

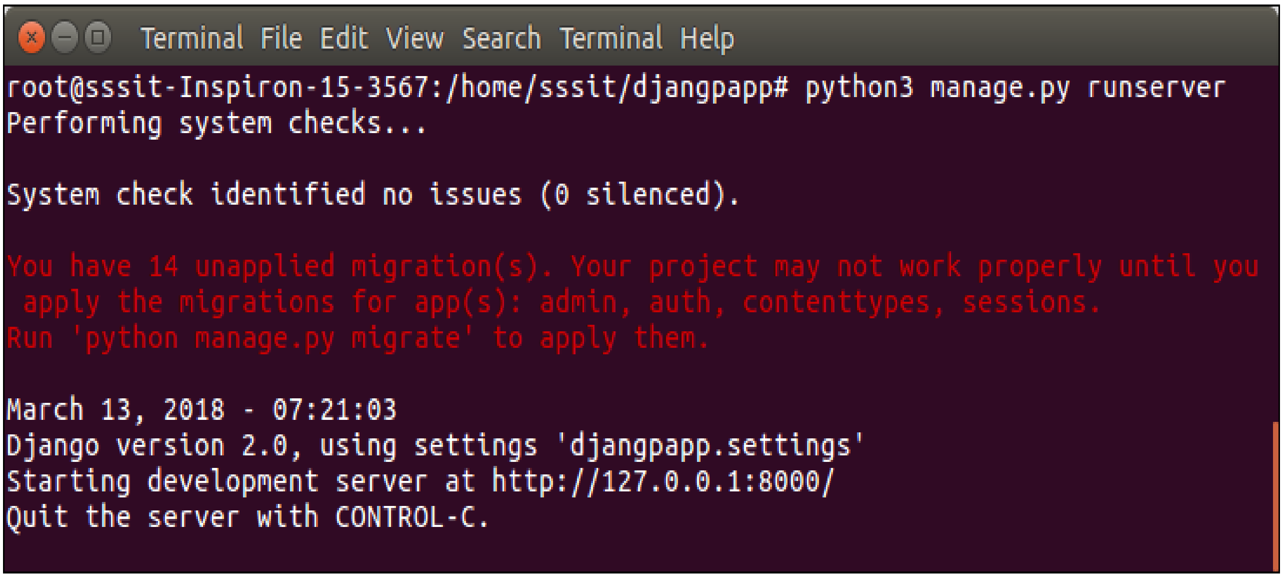
Initially, this project is a default draft which contains all the required files and folders.

Running the Django Project

Django project has a built-in development server which is used to run application instantly without any external web server. It means we don't need of Apache or another web server to run the application in development mode.

To run the application, we can use the following command.

$ python3 manage.py runserver



```
root@sssit-Inspiron-15-3567:/home/sssit/djangpapp# python3 manage.py runserver
Performing system checks...

System check identified no issues (0 silenced).

You have 14 unapplied migration(s). Your project may not work properly until you
 apply the migrations for app(s): admin, auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.

March 13, 2018 - 07:21:03
Django version 2.0, using settings 'djangpapp.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
```

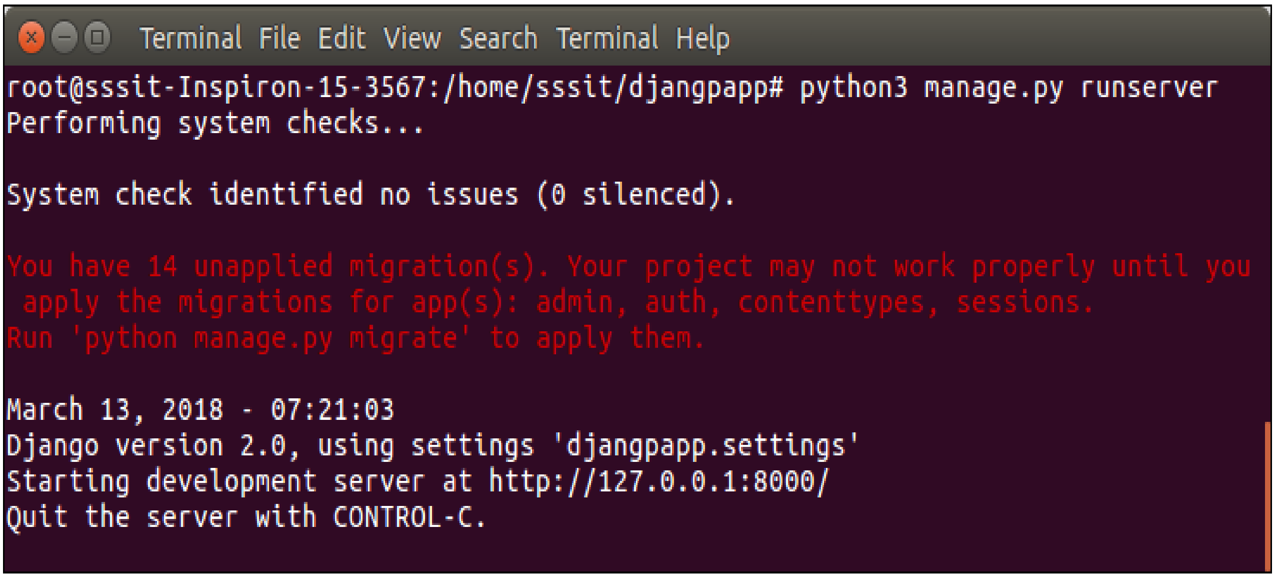
Look server has started and can be accessed at localhost with port 8000. Let's access it using the browser, it looks like the below.

The application is running successfully. Now, we can customize it according to our requirement and can develop a customized web application.

Django Configuration with Apache Web Server

Django uses its built-in development server to run the web application. To start this server, we can use python manage.py runserver command.

This command starts the server which runs on port 8000 and can be accessed at browser by entering localhost:8000. It shows a welcome page of the application.



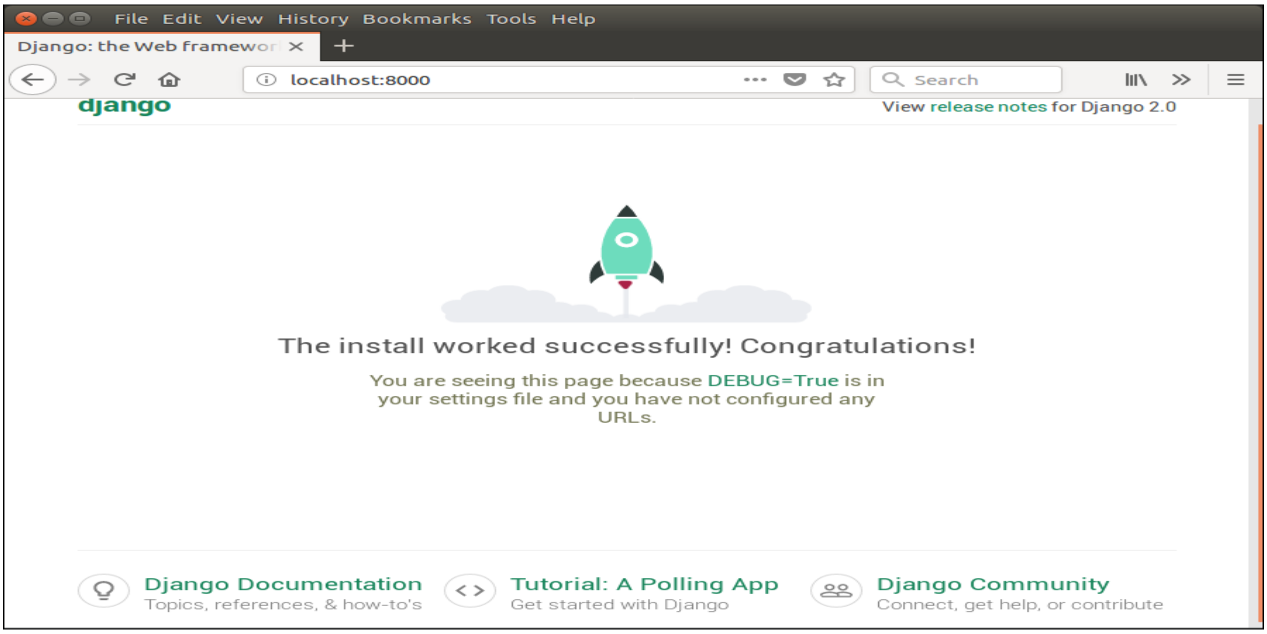
```
root@sssit-Inspiron-15-3567:/home/sssit/djangpapp# python3 manage.py runserver
Performing system checks...

System check identified no issues (0 silenced).

You have 14 unapplied migration(s). Your project may not work properly until you
 apply the migrations for app(s): admin, auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.

March 13, 2018 - 07:21:03
Django version 2.0, using settings 'djangpapp.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
```

And at browser, it can be accessed as below.


File Edit View History Bookmarks Tools Help
Django: the Web framewor
localhost:8000
Search
django
View release notes for Django 2.0
Django Documentation
Topics, references, & how-to's
Tutorial: A Polling App
Get started with Django
Django Community
Connect, get help, or contribute

The install worked successfully! Congratulations!

You are seeing this page because DEBUG=True is in your settings file and you have not configured any URLs.

But if we want to run our application by using **apache server** rather than built-in development server, we need to configure **apache2.conf** file located at **/etc/apache** directory. Add the following code into this file.

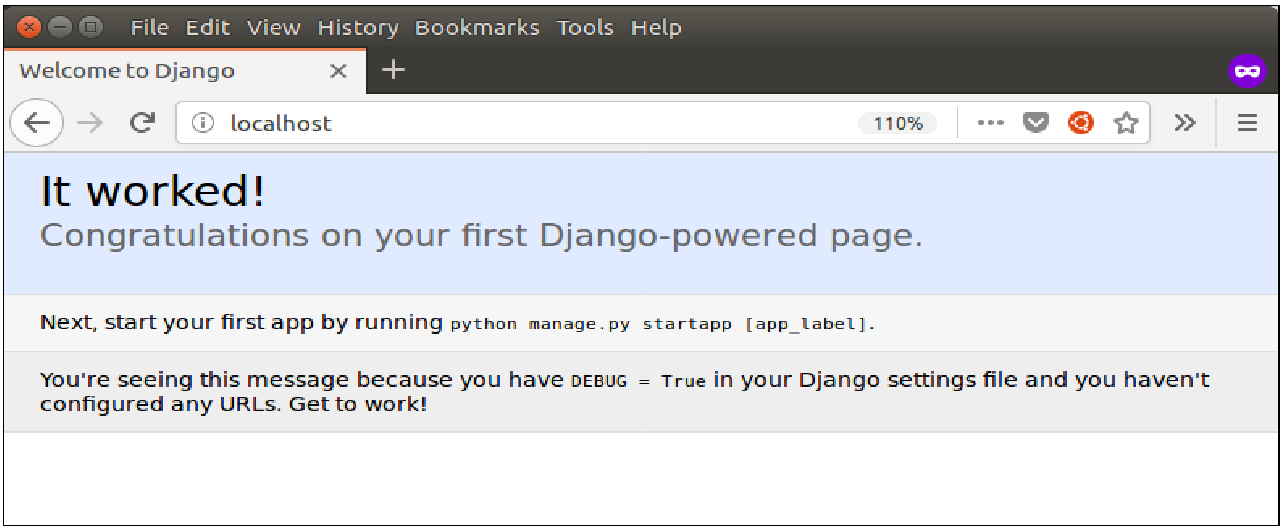
// apache2.conf

```
1.  WSGIScriptAlias / /var/www/html/django7/django7/wsgi.py
2.  WSGIPythonPath /var/www/html/django7/
3.
4.  <Directory /var/www/html/django7>
5.     <Files wsgi.py>
6.               Require all granted
```

7.	</Files>

8. </Directory>

After adding these lines, restart apache server by using the **service apache2 restart** command and then type **localhost** to the browser's address bar. This time, project will run on apache server rather than a built-in server. See, it shows the home page of the application.



It worked!
Congratulations on your first Django-powered page.

Next, start your first app by running `python manage.py startapp [app_label]`.

You're seeing this message because you have `DEBUG = True` in your Django settings file and you haven't configured any URLs. Get to work!

Django Virtual Environment Setup

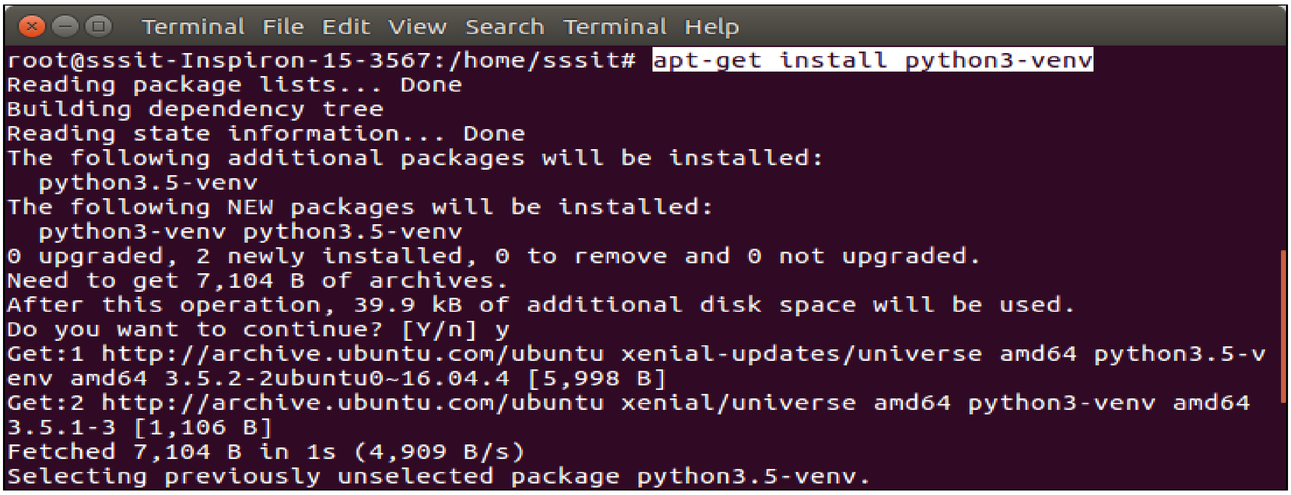
The virtual environment is an environment which is used by Django to execute an application. It is recommended to create and execute a Django application in a separate environment. Python provides a tool **virtualenv** to create an isolated Python environment. We will use this tool to create a virtual environment for our Django application.

To set up a virtual environment, use the following steps.

1. Install Package

First, install **python3-venv** package by using the following command.

$ apt-get install python3-venv

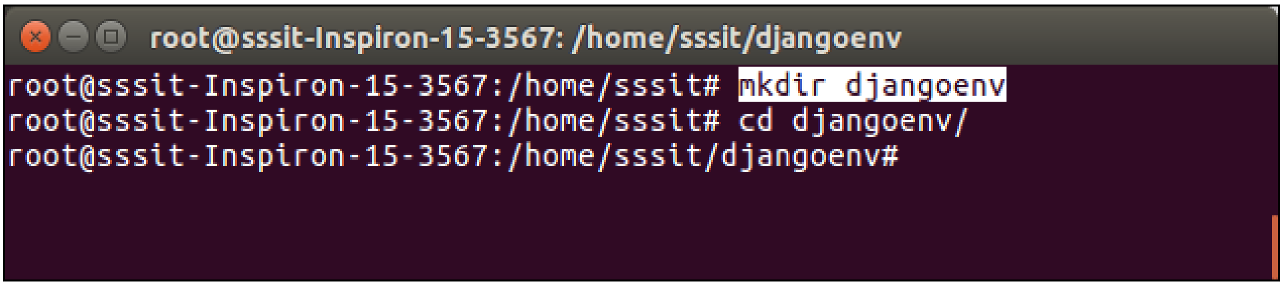


```
root@sssit-Inspiron-15-3567:/home/sssit# apt-get install python3-venv
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3.5-venv
The following NEW packages will be installed:
  python3-venv python3.5-venv
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 7,104 B of archives.
After this operation, 39.9 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu xenial-updates/universe amd64 python3.5-v
env amd64 3.5.2-2ubuntu0~16.04.4 [5,998 B]
Get:2 http://archive.ubuntu.com/ubuntu xenial/universe amd64 python3-venv amd64
3.5.1-3 [1,106 B]
Fetched 7,104 B in 1s (4,909 B/s)
Selecting previously unselected package python3.5-venv.
```

2. Create a Directory

$ mkdir djangoenv

After it, change directory to the newly created directory by using the **cd djangoenv.**



```
root@sssit-Inspiron-15-3567:/home/sssit# mkdir djangoenv
root@sssit-Inspiron-15-3567:/home/sssit# cd djangoenv/
root@sssit-Inspiron-15-3567:/home/sssit/djangoenv#
```

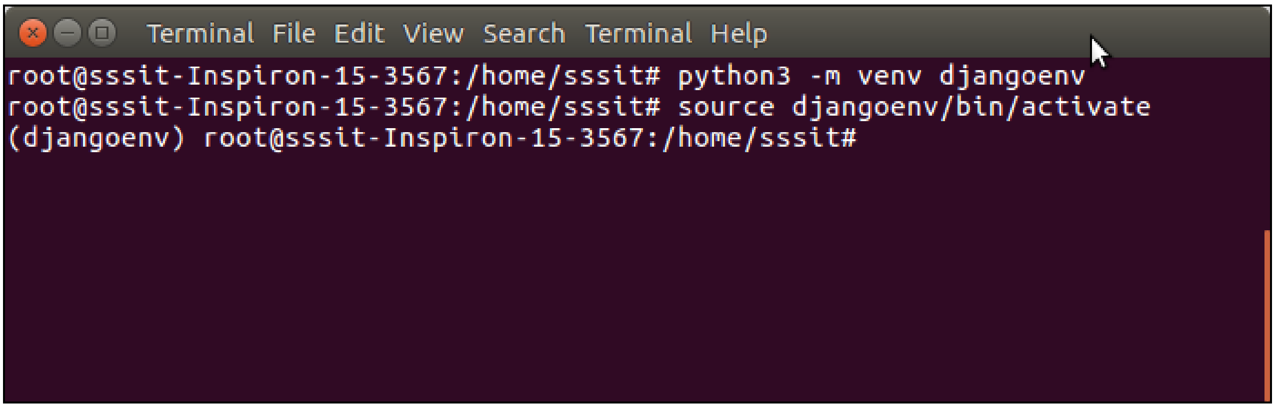
3. Create Virtual Environment

$ python3 -m venv djangoenv

4. Activate Virtual Environment

After creating a virtual environment, activate it by using the following command.

$ source djangoenv/bin/activate



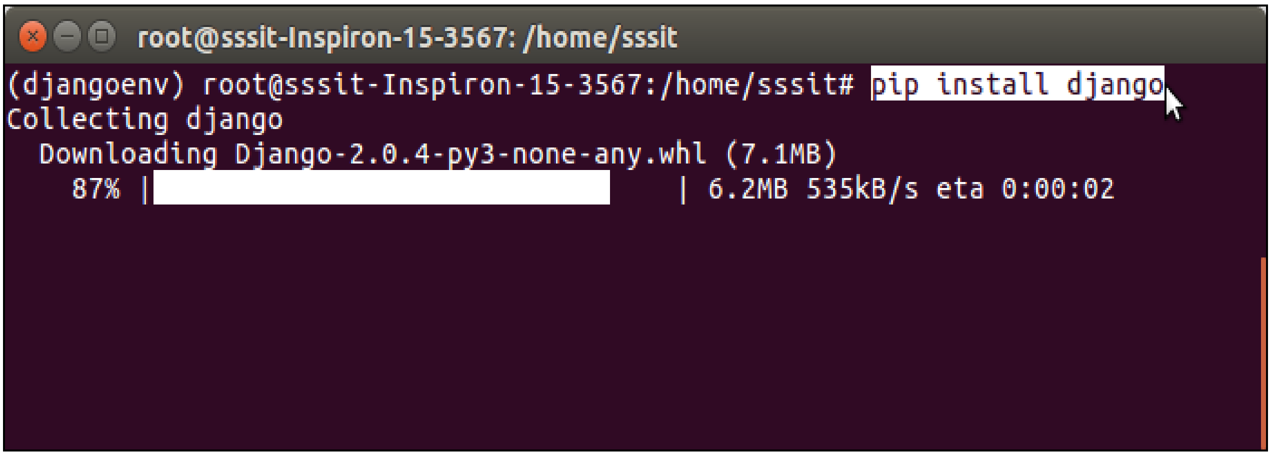
```
root@sssit-Inspiron-15-3567:/home/sssit# python3 -m venv djangoenv
root@sssit-Inspiron-15-3567:/home/sssit# source djangoenv/bin/activate
(djangoenv) root@sssit-Inspiron-15-3567:/home/sssit#
```

Till here, the virtual environment has started. Now, we can use it to create Django application.

Install Django

Install Django in the virtual environment. To install Django, use the following command.

$ pip install django



```
(djangoenv) root@sssit-Inspiron-15-3567:/home/sssit# pip install django
Collecting django
  Downloading Django-2.0.4-py3-none-any.whl (7.1MB)
    87% |                            | 6.2MB 535kB/s eta 0:00:02
```

Django has installed successfully. Now we can create a new project and build new applications in the separate environment

Django Admin Interface

Django provides a built-in admin module which can be used to perform CRUD operations on the models. It reads metadata from the model to provide a quick interface where the user can manage the content of the application. This is a built-in module and designed to perform admin related tasks to the user. Let's see how to activate and use Django's admin module (interface).

The admin app **(django.contrib.admin)** is enabled by default and already added into INSTALLED_APPS section of the settings file.

To access it at browser use '/**admin**/' at a local machine like **localhost:8000/admin/** and it shows the following output:

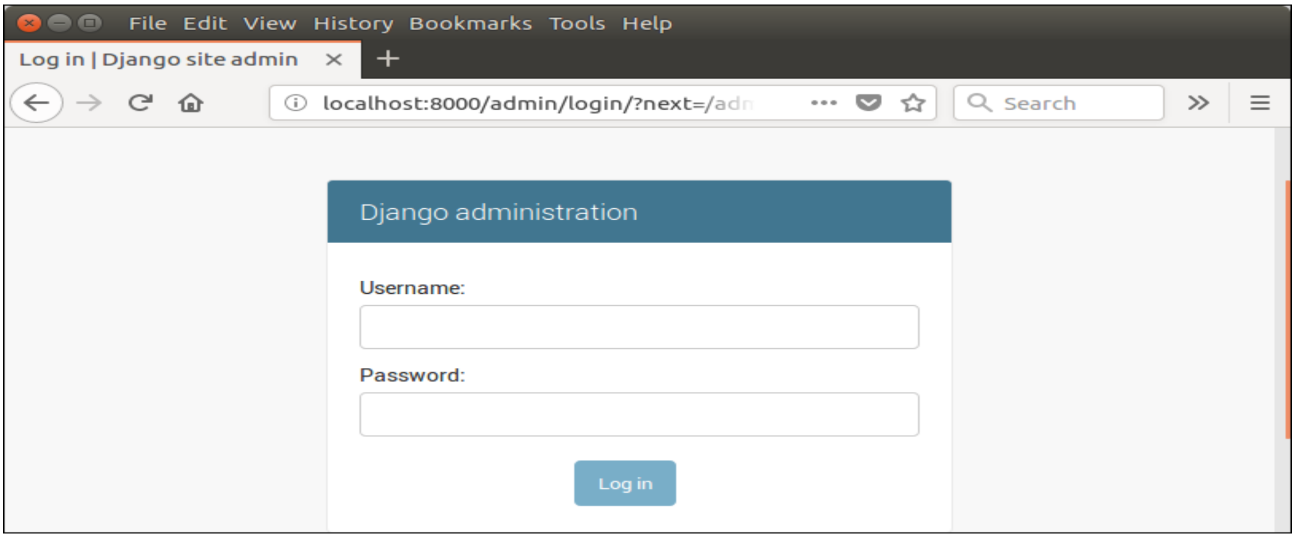
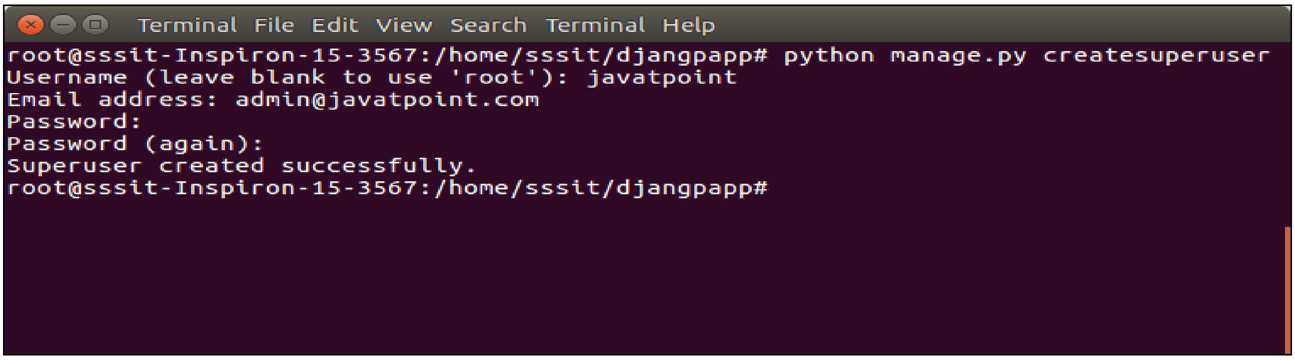

File Edit View History Bookmarks Tools Help
Log in | Django site admin
localhost:8000/admin/login/?next=/adn
Search
Django administration
Username:
Password:
Log in

Fig:4.5 Django Admin Login

It prompts for login credentials if no password is created yet, use the following command to create a user.

Create an Admin User

$ python3 managen.py createsuperuser

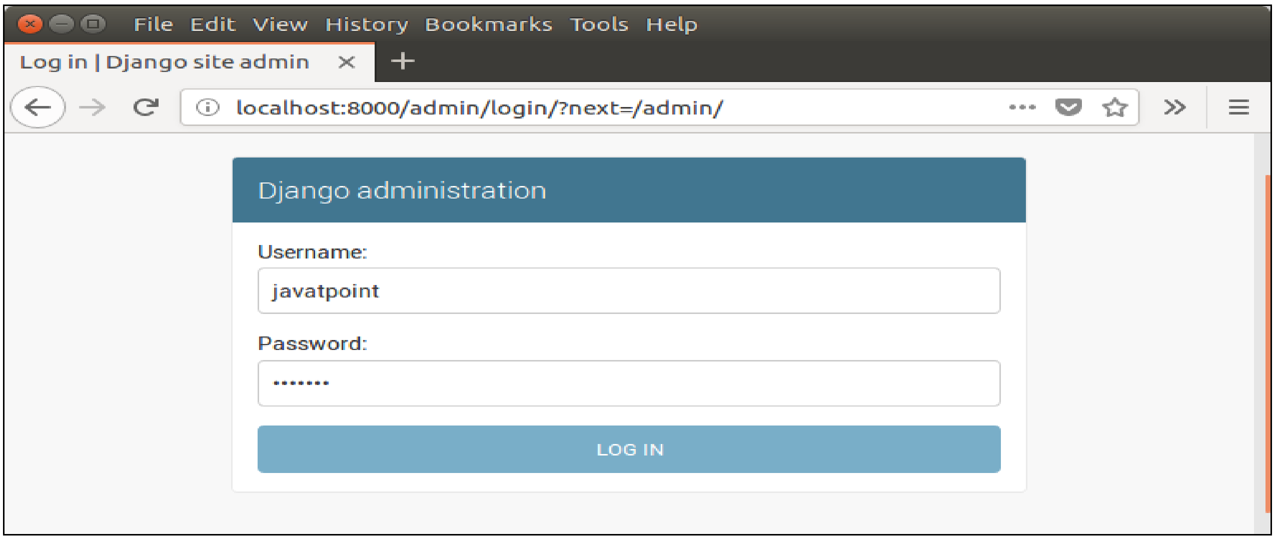


```
root@sssit-Inspiron-15-3567:/home/sssit/djangpapp# python manage.py createsuperuser
Username (leave blank to use 'root'): javatpoint
Email address: admin@javatpoint.com
Password:
Password (again):
Superuser created successfully.
root@sssit-Inspiron-15-3567:/home/sssit/djangpapp#
```

Now start development server and access admin login.

```
$ python3 manage.py runserver
```

Provide created username and password and login.

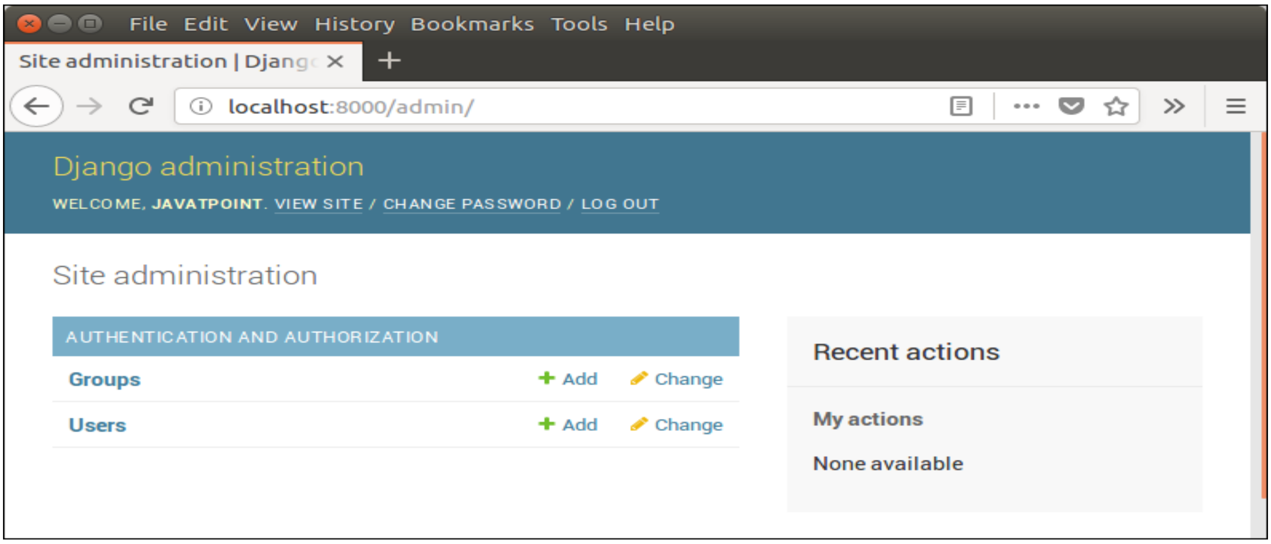

File Edit View History Bookmarks Tools Help
Log in | Django site admin
localhost:8000/admin/login/?next=/admin/
LOG IN

Django administration

Username: javatpoint

Password: •••••••

After login successfully, it shows the following interface.


File Edit View History Bookmarks Tools Help
Site administration | Djang
localhost:8000/admin/
VIEW SITE / CHANGE PASSWORD / LOG OUT

Django administration

WELCOME, JAVATPOINT.

Site administration

AUTHENTICATION AND AUTHORIZATION		
Groups	+ Add	Change
Users	+ Add	Change

Recent actions

My actions

None available

It is a Django Admin Dashboard.

Django App

In the previous topics, we have seen a procedure to create a Django project. Now, in this topic, we will create app inside the created project.

Django application consists of project and app, it also generates an automatic base directory for the app, so we can focus on writing code (business logic) rather than creating app directories. The difference between a project and app is, a project is a collection of configuration files and apps whereas the app is a web application which is written to perform business logic.

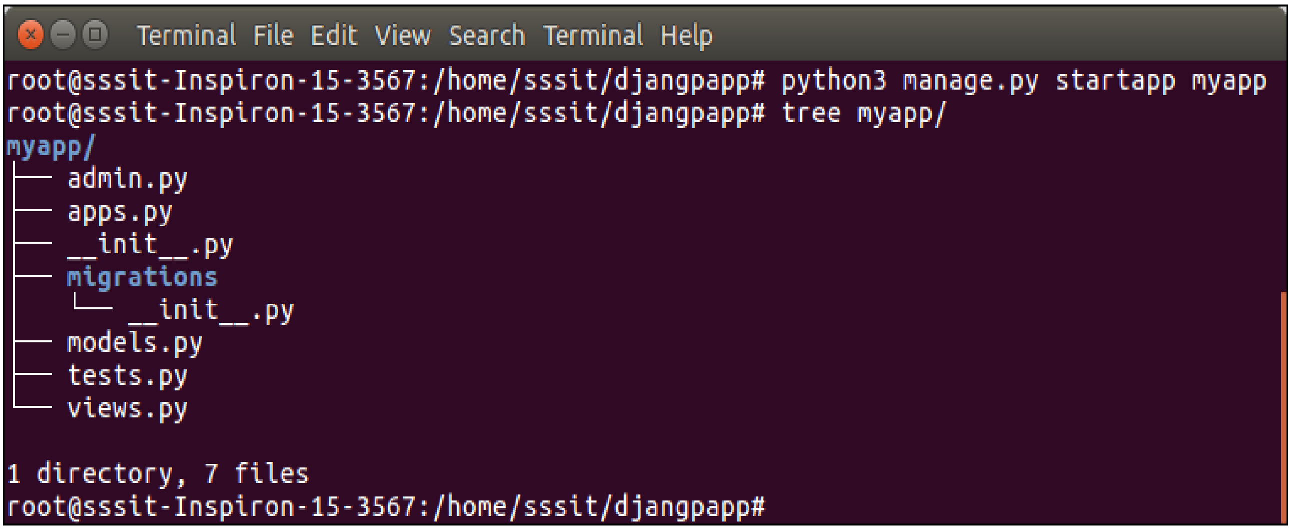
Creating an App

To create an app, we can use the following command.

```
$ python3 manage.py startapp appname
```

Django App Example

$ python3 manage.py startapp myapp



```
root@sssit-Inspiron-15-3567:/home/sssit/djangpapp# python3 manage.py startapp myapp
root@sssit-Inspiron-15-3567:/home/sssit/djangpapp# tree myapp/
myapp/
├── admin.py
├── apps.py
├── __init__.py
├── migrations
│   └── __init__.py
├── models.py
├── tests.py
└── views.py

1 directory, 7 files
root@sssit-Inspiron-15-3567:/home/sssit/djangpapp#
```

See the directory structure of the created app, it contains the **migrations** folder to store migration files and model to write business logic. Initially, all the files are empty, no code is available but we can use these to implement business logic on the basis of the MVC design pattern. To run this application, we need to make some significant changes which display **hello world** message on the browser.

Open **views.py** file in any text editor and write the given code to it and do the same for **urls.py** file too.

// **views.py**

```
from django.shortcuts import render

# Create your views here.
from django.http import HttpResponse

def hello(request):
    return HttpResponse("<h2>Hello, Welcome to Django!</h2>")
```

// **urls.py**

```
from django.contrib import admin
from django.urls import path
from myapp import views

urlpatterns = [
    path('admin/', admin.site.urls),
```

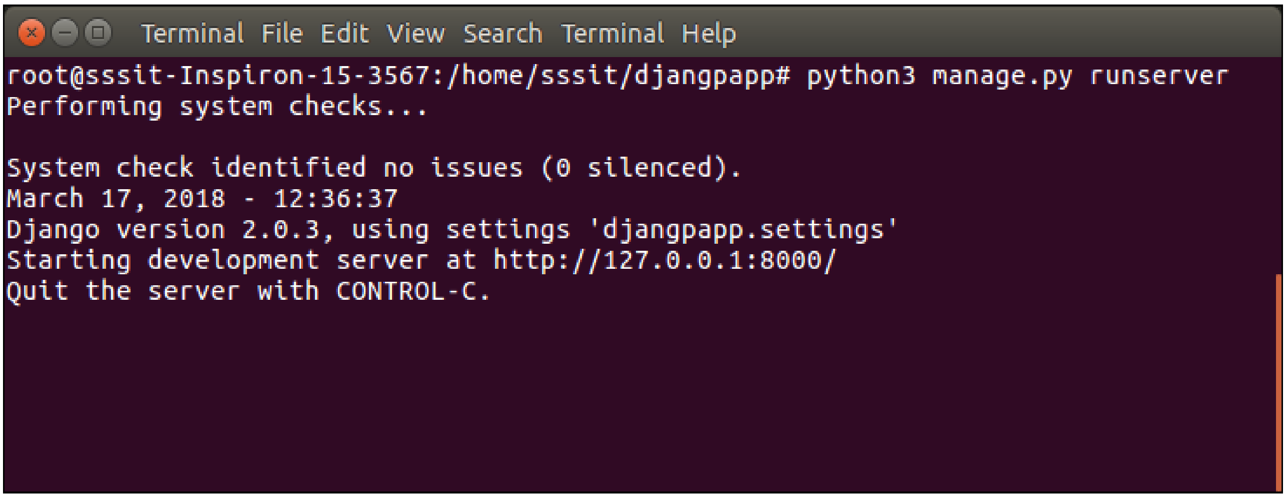
7.	path('hello/', views.hello),

8.]

We have made changes in two files of the application. Now, let's run the it by using the following command. This command will start the server at port 8000.

Run the Application

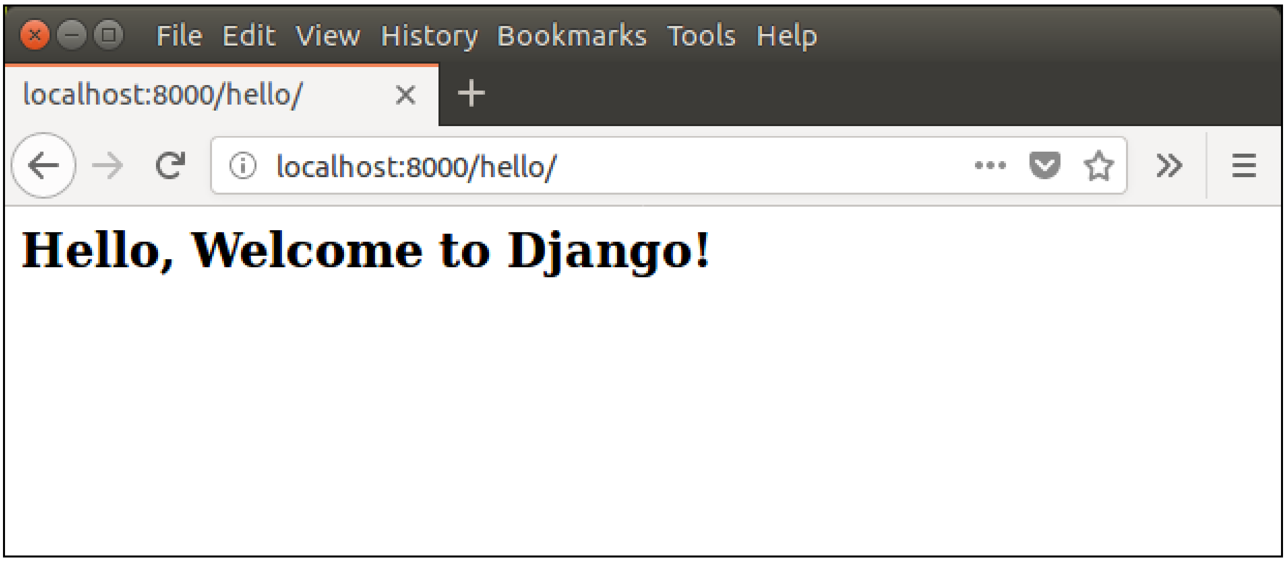
$ python3 manage.py runserver



```
root@sssit-Inspiron-15-3567:/home/sssit/djangpapp# python3 manage.py runserver
Performing system checks...

System check identified no issues (0 silenced).
March 17, 2018 - 12:36:37
Django version 2.0.3, using settings 'djangpapp.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
```

Open any web browser and enter the URL **localhost:8000/hello**. It will show the output given below.



Hello, Welcome to Django!

Django MVT

The MVT (Model View Template) is a software design pattern. It is a collection of three important components Model View and Template. The Model helps to handle database. It is a data access layer which handles the data. The Template is a presentation layer which handles User Interface part completely. The View is used to execute the business logic and interact with a model to carry data and renders a template. Although Django follows MVC pattern but maintains it?s own conventions. So, control is handled by the framework itself. There is no separate controller and complete application is based on Model View and Template. That?s why it is called MVT application. See the following graph that shows the MVT based control flow.

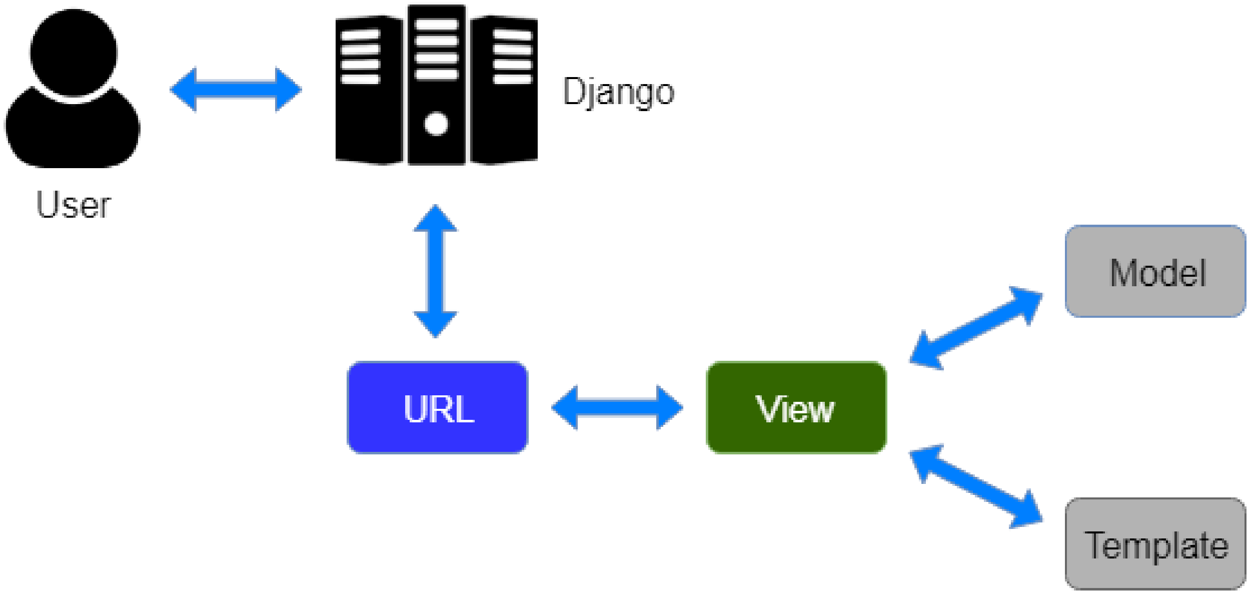


Fig:4.6 MVT Based Control Flow

Here, a user **requests** for a resource to the Django, Django works as a controller and check to the available resource in URL. If URL maps, **a view is called** that interact with model and template, it renders a template.

Django Views

A view is a place where we put our business logic of the application. The view is a python function which is used to perform some business logic and return a response to the user. This response can be the HTML contents of a Web page, or a redirect, or a 404 error.

All the view function are created inside the **views.py** file of the Django app.

Django View Simple Example

//views.py

```
import datetime
# Create your views here.
from django.http import HttpResponse
def index(request):
    now = datetime.datetime.now()
    html = "<html><body><h3>Now time is %s.</h3></body></html>" % now
    return HttpResponse(html)    # rendering the template in HttpResponse
```

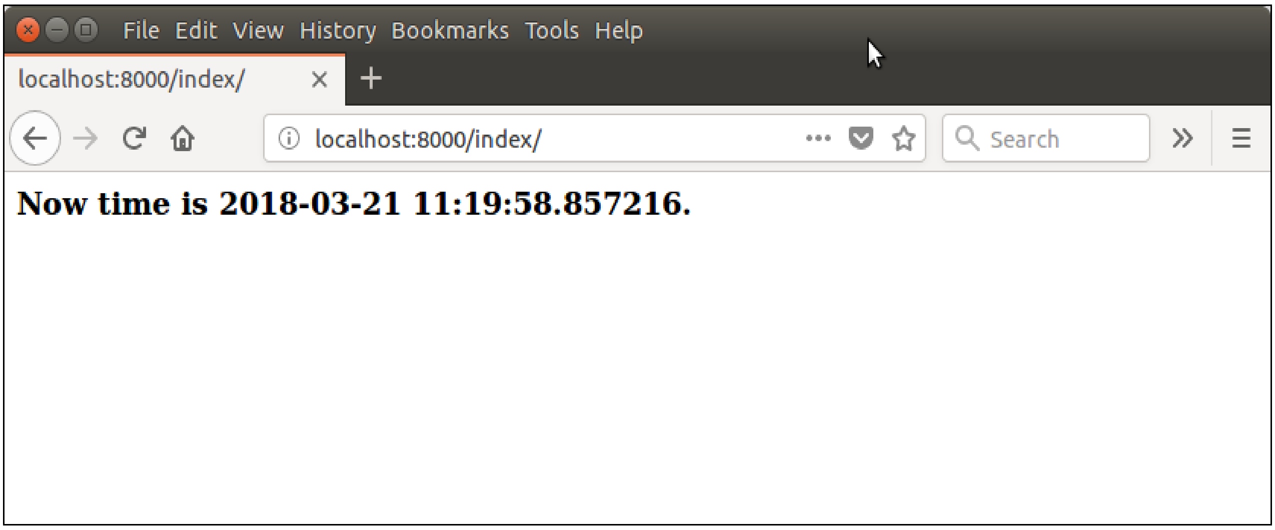
Let's step through the code.

First, we will import DateTime library that provides a method to get current date and time and HttpResponse class. Next, we define a view function index that takes HTTP request and respond back.

View calls when gets mapped with URL in **urls.py.** For example

path('index/', views.index),

Output:



Now time is 2018-03-21 11:19:58.857216.

4.2 Back End Implementation

What is MySQL

MySQL is a fast, easy to use relational database. It is currently the most popular open-source database. It is very commonly used in conjunction with PHP scripts to create powerful and dynamic server-side applications. MySQL is used for many small and big businesses. It is developed, marketed and supported by MySQL AB, a Swedish company. It is written in C and C++.

MySQL Create Database

A database is a collection of data. MySQL allows us to store and retrieve the data from the database in a efficient way. In MySQL, we can create a database using the CREATE DATABASE statement. But, if database already exits, it throws an error. To avoid the error, we can use the IF NOT EXISTS option with the CREATE DATABASE statement. You can create a MySQL database by using MySQL Command Line Client. Open the MySQL console and write down password, if you set one while installation. You will get the following:

mysql create database 1

Now you are ready to create database

Syntax: CREATE DATABASE database_name;

Let's take an example to create a database name "employees"

CREATE DATABASE employees;

MySQL Drop Database

You can drop/delete/remove a MySQL database easily with the MySQL DROP DATABASE command. It deletes all the tables of the database along with the database permanently. It throws an error, if the database is not available. We can use the IF EXISTS option with the DROP DATABASE statement. It returns the numbers of tables which are deleted through the DROP DATABASE statement. We should be careful while deleting any database because we will loose all the data available in the database.

Syntax: DROP DATABASE database_name;

Example: Let's take an example to drop a database name "employees"

DROP DATABASE employees;

MySQL CREATE TABLE

The MySQL CREATE TABLE command is used to create a new table into the database. A table creation command requires three things:

Name of the table

Names of fields

Definitions for each field

CREATE TABLE table_name (column_name column_type...);

next ??prev

MySQL CREATE TABLE

The MySQL CREATE TABLE command is used to create a new table into the database. A table creation command requires three things:

Name of the table

Names of fields

Definitions for each field

Syntax:

Following is a generic syntax for creating a MySQL table in the database.

CREATE TABLE table_name (column_name column_type...);

Example:

Here, we will create a table named "cus_tbl" in the database "customers".

CREATE TABLE cus_tbl(

cus_id INT NOT NULL AUTO_INCREMENT,

```
cus_firstname VARCHAR(100) NOT NULL,
cus_surname VARCHAR(100) NOT NULL,
  PRIMARY KEY ( cus_id )
);
```

MySQL Queries

A list of commonly used MySQL queries to create database, use database, create table, insert record, update record, delete record, select record, truncate table and drop table are given below.

1) MySQL Create Database

MySQL create database is used to create database. For example

```
create database db1;
```

MySQL INSERT Statement

MySQL INSERT statement is used to insert data in MySQL table within the database. We can insert single or multiple records using a single query in MySQL.

```
INSERT INTO table_name ( field1, field2,...fieldN )
VALUES
( value1, value2,...valueN );
INSERT INTO table_name VALUES ( value1, value2,...valueN );
```

MySQL UPDATE Query

MySQL UPDATE statement is used to update data of the MySQL table within the database. In real life scenario, records are changed over the period of time. So, we need to make changes in the values of the tables also. To do so, we need to use the UPDATE statement.

The UPDATE statement is used with the SET, and WHERE clauses. The SET clause is used to change the values of the specified column. We can update single or multiple columns at a time. The WHERE clause is used to specify the condition, but it is optional.

Syntax:

Following is a generic syntax of UPDATE command to modify data into the MySQL table:

```
UPDATE table_name
SET field1=new-value1, field2=new-value2, ...
[WHERE Clause]
```

MySQL DELETE Statement

MySQL DELETE statement is used to delete data from the MySQL table within the database. By using delete statement, we can delete records on the basis of conditions.

Syntax:

```
DELETE FROM table_name
WHERE
(Condition specified);
```

Example:

```
DELETE FROM cus_tbl
WHERE cus_id = 6;
```

MySQL ALTER Table

MySQL ALTER statement is used when you want to change the name of your table or any table field. It is also used to add or delete an existing column in a table.

The ALTER statement is always used with "ADD", "DROP" and "MODIFY" commands according to the situation.

1) ADD a column in the table

Syntax:

```
ALTER TABLE table_name
ADD new_column_name column_definition
[ FIRST | AFTER column_name ];
```

Parameters

table_name: It specifies the name of the table that you want to modify.

new_column_name: It specifies the name of the new column that you want to add to the table.

column_definition: It specifies the data type and definition of the column (NULL or NOT NULL, etc).

FIRST | AFTER column_name: It is optional. It tells MySQL where in the table to create the column. If this parameter is not specified, the new column will be added to the end of the table.

Example:

In this example, we add a new column "cus_age" in the existing table "cus_tbl".

Use the following query to do this:

```
ALTER TABLE cus_tbl
ADD cus_age varchar(40) NOT NULL;
```

MySQL JOINS

MySQL JOINS are used with SELECT statement. It is used to retrieve data from multiple tables. It is performed whenever you need to fetch records from two or more tables.

There are three types of MySQL joins:

MySQL INNER JOIN (or sometimes called simple join)

MySQL LEFT OUTER JOIN (or sometimes called LEFT JOIN)

MySQL RIGHT OUTER JOIN (or sometimes called RIGHT JOIN)

MySQL Inner JOIN (Simple Join)

The MySQL INNER JOIN is used to return all rows from multiple tables where the join condition is satisfied. It is the most common type of join.

Syntax:

```
SELECT columns
FROM table1
INNER JOIN table2
ON table1.column = table2.column;
```

MySQL count() Function

The MySQL count() function is used to return the count of an expression. It is used when you need to count some records of your table.

Syntax:

```
SELECT COUNT (aggregate_expression)
FROM table_name
[WHERE conditions];
```

Parameter explanation

aggregate_expression: It specifies the column or expression whose NON-NULL values will be counted.

table_name: It specifies the tables, from where you want to retrieve records. There must be at least one table listed in the FROM clause.

WHERE conditions: It is optional. It specifies the conditions that must be fulfilled for the records to be selected.

4.3 SOURCE CODE

manage.py

```
#!/usr/bin/env python
import os
import sys
if __name__ == "__main__":
    os.environ.setdefault("DJANGO_SETTINGS_MODULE", "cyber_security_alert.settings")
    try:
        from django.core.management import execute_from_command_line
    except ImportError:
        # The above import may fail for some other reason. Ensure that the
        # issue is really that Django is missing to avoid masking other
        # exceptions on Python 2.
        try:
            import django
        except ImportError:
            raise ImportError(
                "Couldn't import Django.Are you sure it's installed and "
                "available on your PYPATH environment variable? Did you "
                "forget to activate a virtual environment?"
            )
        raise
    execute_from_command_line(sys.argv)
```

settings.py

```
"""
Django settings for cyber_security_alert project.
Generated by 'django-admin startproject' using Django 1.11.5.
For more information on this file, see
https://docs.djangoproject.com/en/1.11/topics/settings/
For the full list of settings and their values, see
https://docs.djangoproject.com/en/1.11/ref/settings/
"""
import os
```

```
# Build paths inside the project like this: os.path.join(BASE_DIR, ...)
BASE_DIR = os.path.dirname(os.path.dirname(os.path.abspath(__file__)))


# Quick-start development settings - unsuitable for production
# See https://docs.djangoproject.com/en/1.11/howto/deployment/checklist/
# SECURITY WARNING: keep the secret key used in production secret!
SECRET_KEY = 'gn-jzi2u3%gw+olpxfrd%ye6210z3=$+(r@c5ly(%8j2$5)k77'
# SECURITY WARNING: don't run with debug turned on in production!
DEBUG = True
ALLOWED_HOSTS = []
# Application definition
INSTALLED_APPS = [
    'django.contrib.admin',
    'django.contrib.auth',
    'django.contrib.contenttypes',
    'django.contrib.sessions',
    'django.contrib.messages',
    'django.contrib.staticfiles',
    'cyber_alert',
    'admins'
]
MIDDLEWARE = [
    'django.middleware.security.SecurityMiddleware',
    'django.contrib.sessions.middleware.SessionMiddleware',
    'django.middleware.common.CommonMiddleware',
    'django.middleware.csrf.CsrfViewMiddleware',
    'django.contrib.auth.middleware.AuthenticationMiddleware',
    'django.contrib.messages.middleware.MessageMiddleware',
   'django.middleware.clickjacking.XFrameOptionsMiddleware',
]
ROOT_URLCONF = 'cyber_security_alert.urls'
TEMPLATES = [
    {
        'BACKEND': 'django.template.backends.django.DjangoTemplates',
        'DIRS': [((os.path.join(BASE_DIR,'assests/templates')))],
        'APP_DIRS': True,
        'OPTIONS': {
            'context_processors': [
                'django.template.context_processors.debug',
                'django.template.context_processors.request',
                'django.contrib.auth.context_processors.auth',
                'django.contrib.messages.context_processors.messages',
            ],
        },
    },
]
WSGI_APPLICATION = 'cyber_security_alert.wsgi.application'
# Database
# https://docs.djangoproject.com/en/1.11/ref/settings/#databases
DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.mysql',
        'NAME': 'alarm',
        'USER': 'root',
        'PASSWORD': '',
        'HOST': '127.0.0.1',
        'PORT': '3306',
    }
}
# Password validation
# https://docs.djangoproject.com/en/1.11/ref/settings/#auth-password-validators
AUTH_PASSWORD_VALIDATORS = [
    {
        'NAME': 'django.contrib.auth.password_validation.UserAttributeSimilarityValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.MinimumLengthValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.CommonPasswordValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.NumericPasswordValidator',
    },
]
# Internationalization
# https://docs.djangoproject.com/en/1.11/topics/i18n/
LANGUAGE_CODE = 'en-us'
TIME_ZONE = 'UTC'
USE_I18N = True
USE_L10N = True
USE_TZ = True
# Static files (CSS, JavaScript, Images)
# https://docs.djangoproject.com/en/1.11/howto/static-files/
STATIC_URL = '/static/'
STATICFILES_DIRS= [os.path.join(BASE_DIR, 'assests/static')]
MEDIA_URL = '/media/'
MEDIA_ROOT = os.path.join(BASE_DIR, 'assests/media')
```

Urls.py

```
"""cyber_security_alert URL Configuration
The `urlpatterns` list routes URLs to views. For more information please see:
    https://docs.djangoproject.com/en/1.11/topics/http/urls/
Examples:
Function views
    1. Add an import:  from my_app import views
    2. Add a URL to urlpatterns:  url(r'^$', views.home, name='home')
Class-based views
    1. Add an import:  from other_app.views import Home
    2. Add a URL to urlpatterns:  url(r'^$', Home.as_view(), name='home')
```

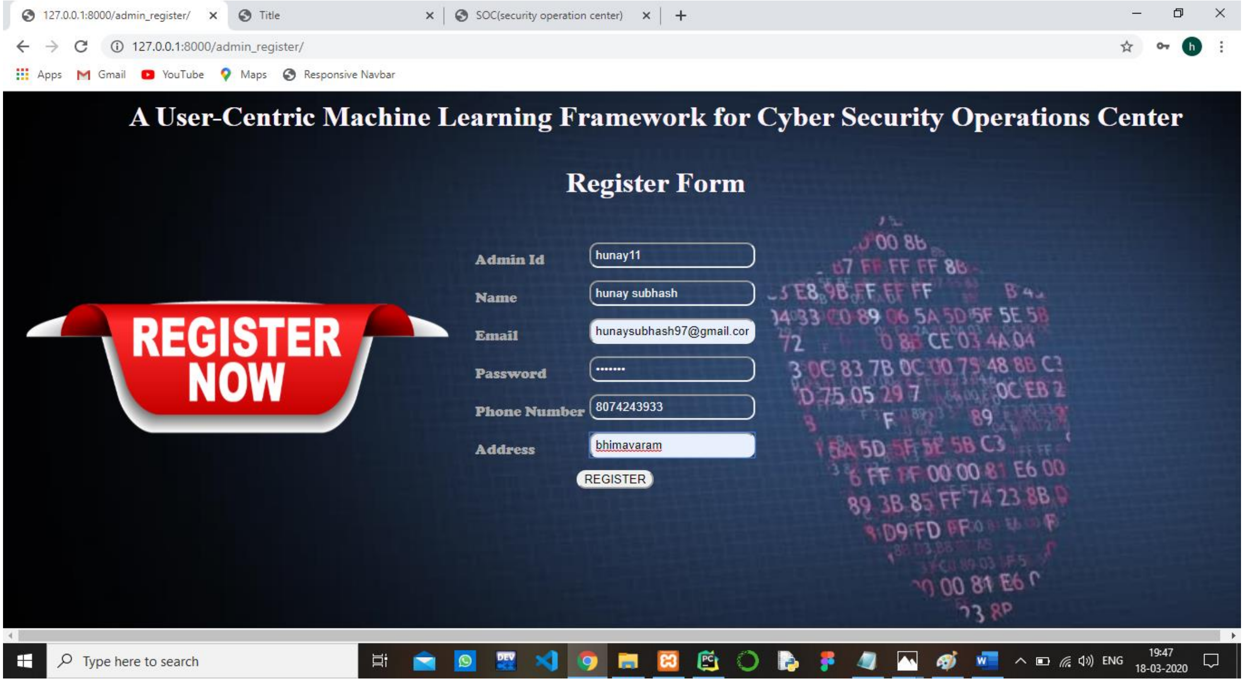
```
Including another URLconf
    1. Import the include() function: from django.conf.urls import url, include
    2. Add a URL to urlpatterns:  url(r'^blog/', include('blog.urls'))
"""
from django.conf.urls import url
from django.contrib import admin
from cyber_alert import views as alert_view
from admins import views as admin_view
urlpatterns = [
    url(r'^admin/', admin.site.urls),
    url(r'^$', alert_view.admin_login, name="admin_login"),
    url(r'^admin_register/$', alert_view.admin_register, name="admin_registe"),
    url(r'^giver_transaction/$', alert_view.giver_transaction, name="giver_transaction"),
    url(r'^analyze_page/$', alert_view.analyze_page, name="analyze_page"),
    url(r'^viewer/(?P<chart_type>\w+)', alert_view.viewer, name="viewer"),
    url(r'^update/$', alert_view.update, name="update"),
    url(r'^logout_page/$', alert_view.logout_page, name="logout_page"),
    url(r'^mydetails/$', alert_view.mydetails, name="mydetails"),
    url(r'^show/$', alert_view.show, name="show"),
    url(r'^receivealert/$', alert_view.receivealert, name="receivealert"),
    url(r'^admins/admin_page/$', admin_view.admin_page, name="admin_page"),
    url(r'^admins/analyze/$', admin_view.analyze, name="analyze"),
    url(r'^admins/adlogout/$', admin_view.adlogout, name="adlogout"),
    url(r'^admins/charts/(?P<chart_type>\w+)', admin_view.charts,name="charts"),
    url(r'^admins/riskuser/$',admin_view.riskuser, name="riskuser"),
    url(r'^admins/riskalert/(?P<tuser>\d+)$',admin_view.riskalert, name="riskalert"),
```

models.py

```
from tkinter import CASCADE
from django.db import models
# Create your models here.
class AdminRegister(models.Model):
    adminid=models.CharField(max_length=50)
    name= models.CharField(max_length=100)
    email=models.EmailField(max_length=50)
    password = models.CharField(max_length=50)
    phoneno=models.CharField(max_length=50)
    address=models.CharField(max_length=50)
class GiverTransaction(models.Model):
    userid= models.ForeignKey(AdminRegister,on_delete=models.CASCADE)
    name = models.CharField(max_length=50)
    aadharno = models.CharField(max_length=50)
    address = models.CharField(max_length=500)
    mobileno = models.CharField(max_length=50)
    bankname = models.CharField(max_length=50)
    accountno = models.CharField(max_length=50)
    branchname = models.CharField(max_length=50)
    amount = models.IntegerField()
    ifsccode = models.CharField(max_length=50)
    micrcode = models.CharField(max_length=50)
    date = models.CharField(max_length=50)
    day = models.CharField(max_length=50)
    month = models.CharField(max_length=50)
    year = models.CharField(max_length=50)
    time = models.CharField(max_length=50)
    transationid = models.CharField(max_length=50)
    countone=models.IntegerField(default=0)
```

4.4 Output Screens

User Registration Page



127.0.0.1:8000/admin_register/

A User-Centric Machine Learning Framework for Cyber Security Operations Center

Register Form

Admin Id: hunay11

Name: hunay subhash

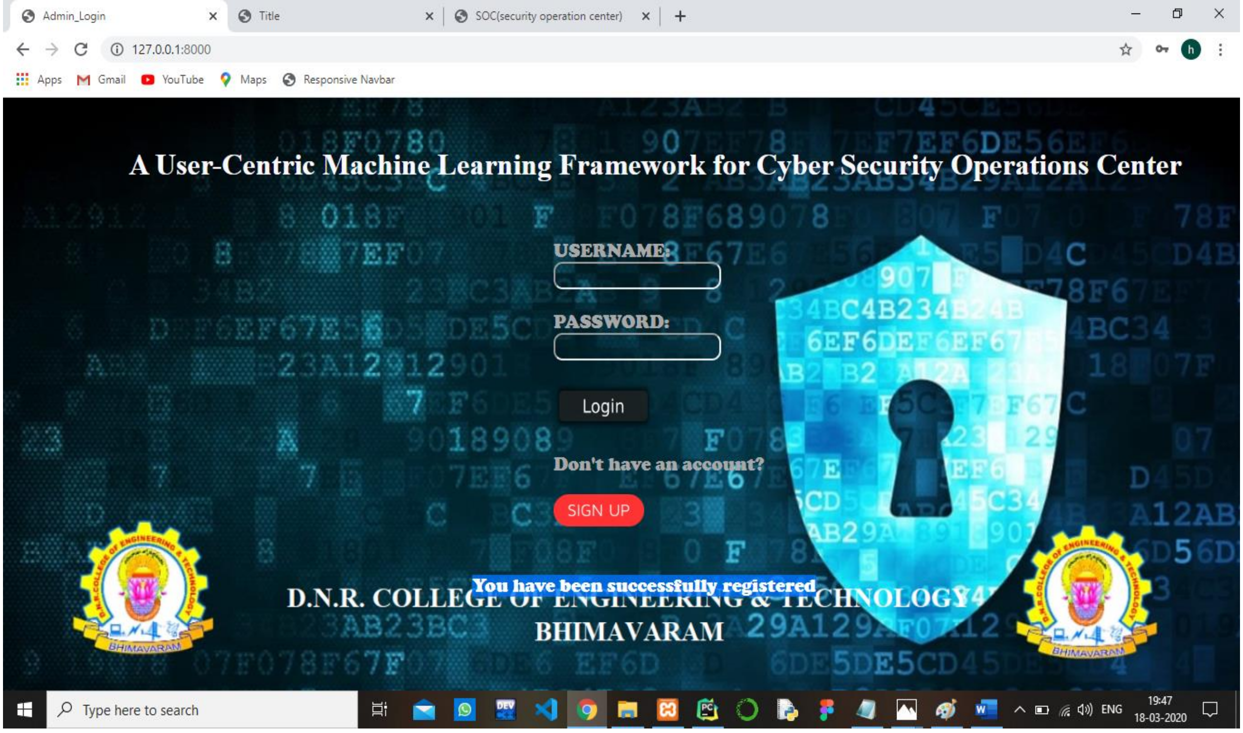
Email: hunaysubhash97@gmail.cor

Password: •••••••

Phone Number: 8074243933

Address: bhimavaram

User Login Page



127.0.0.1:8000

A User-Centric Machine Learning Framework for Cyber Security Operations Center

USERNAME:

PASSWORD:

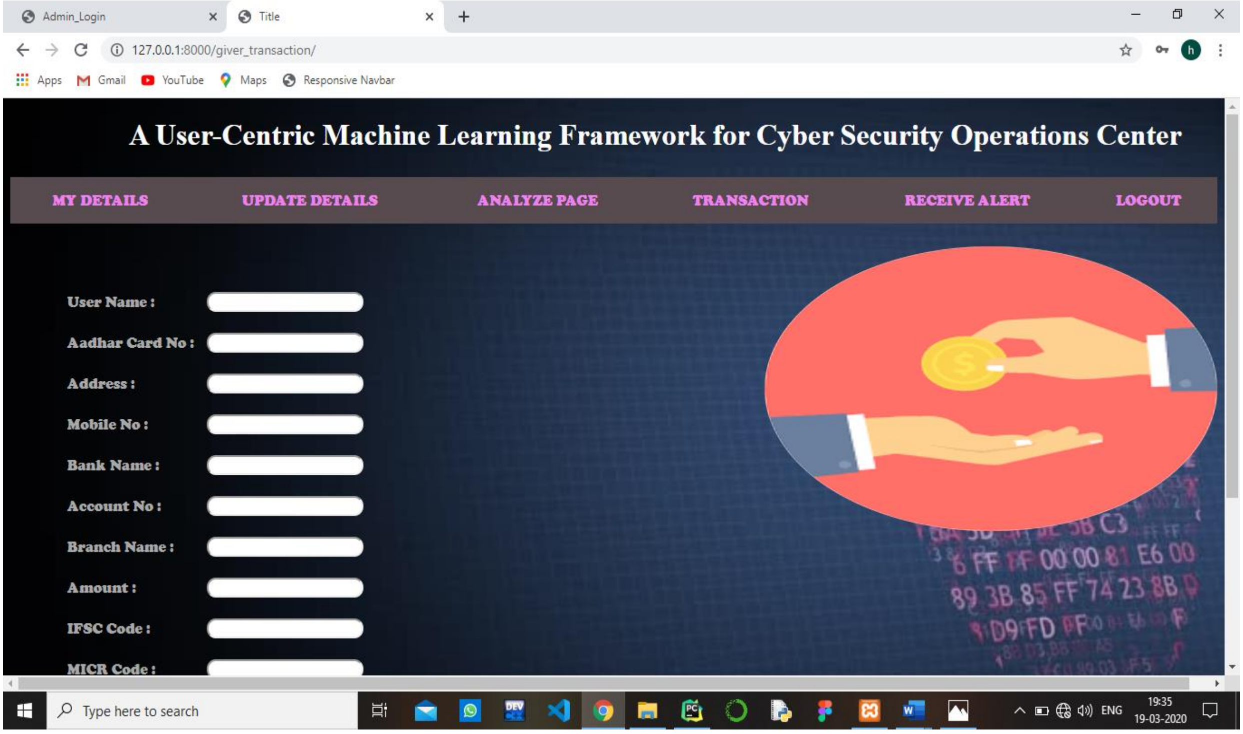
Don't have an account?

You have been successfully registered

D.N.R. COLLEGE OF ENGINEERING & TECHNOLOGY

BHIMAVARAM

Transaction Page



A User-Centric Machine Learning Framework for Cyber Security Operations Center

User Name :

Aadhar Card No :

Address :

Mobile No :

Bank Name :

Account No :

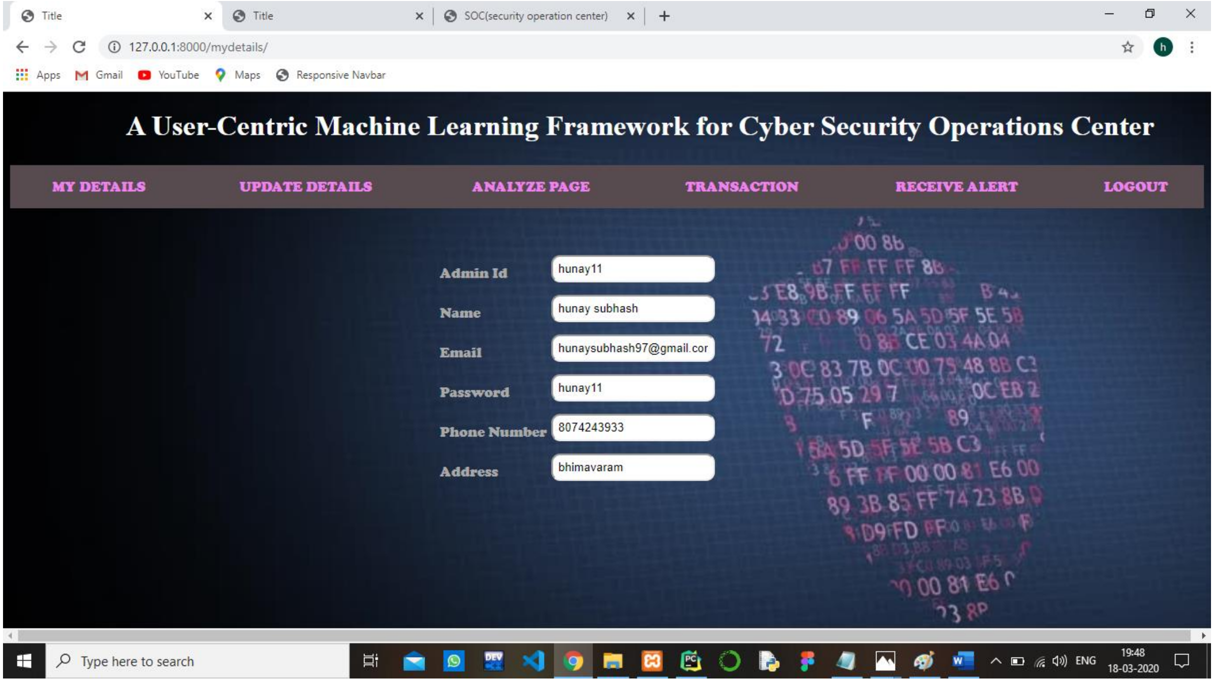
Branch Name :

Amount :

IFSC Code :

MICR Code :

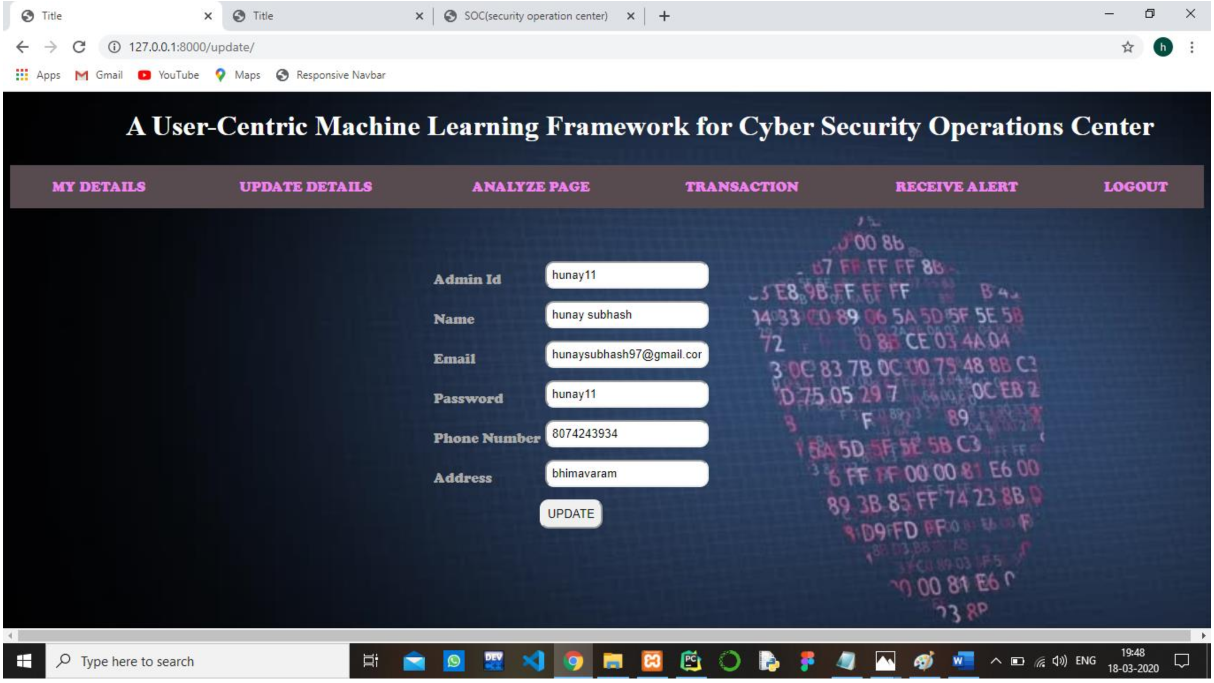
User Details Page



A User-Centric Machine Learning Framework for Cyber Security Operations Center

Admin Id	hunay11
Name	hunay subhash
Email	hunaysubhash97@gmail.cor
Password	hunay11
Phone Number	8074243933
Address	bhimavaram

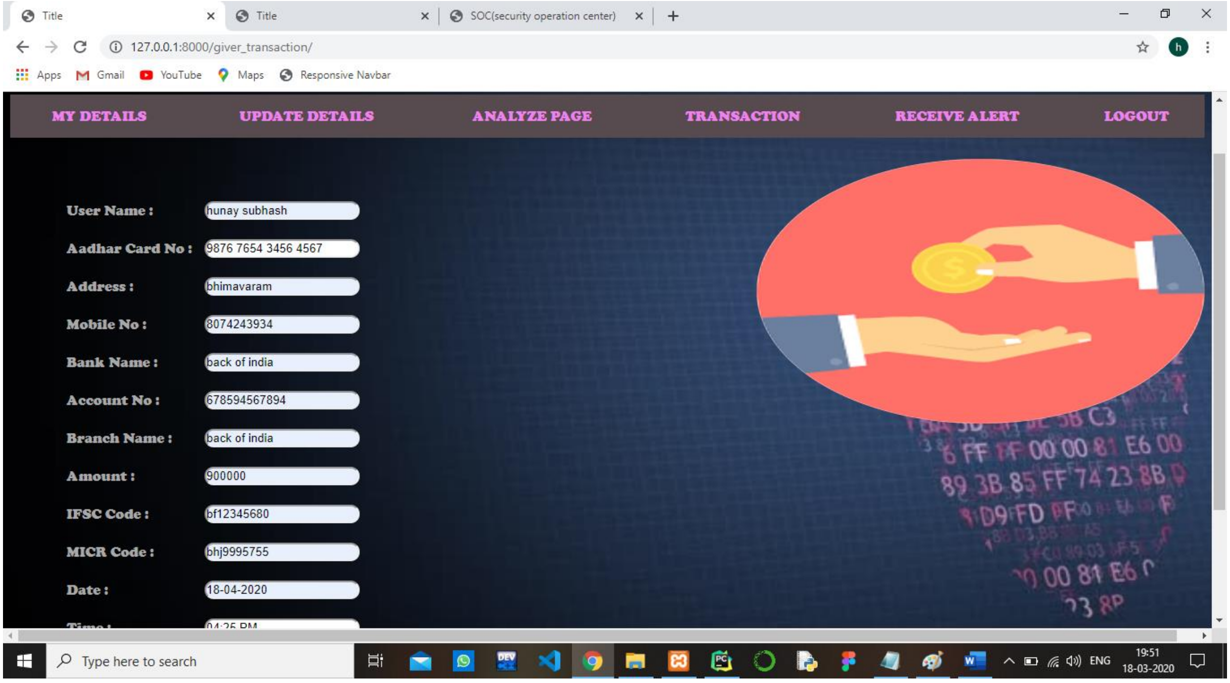
User Details Update Page



A User-Centric Machine Learning Framework for Cyber Security Operations Center

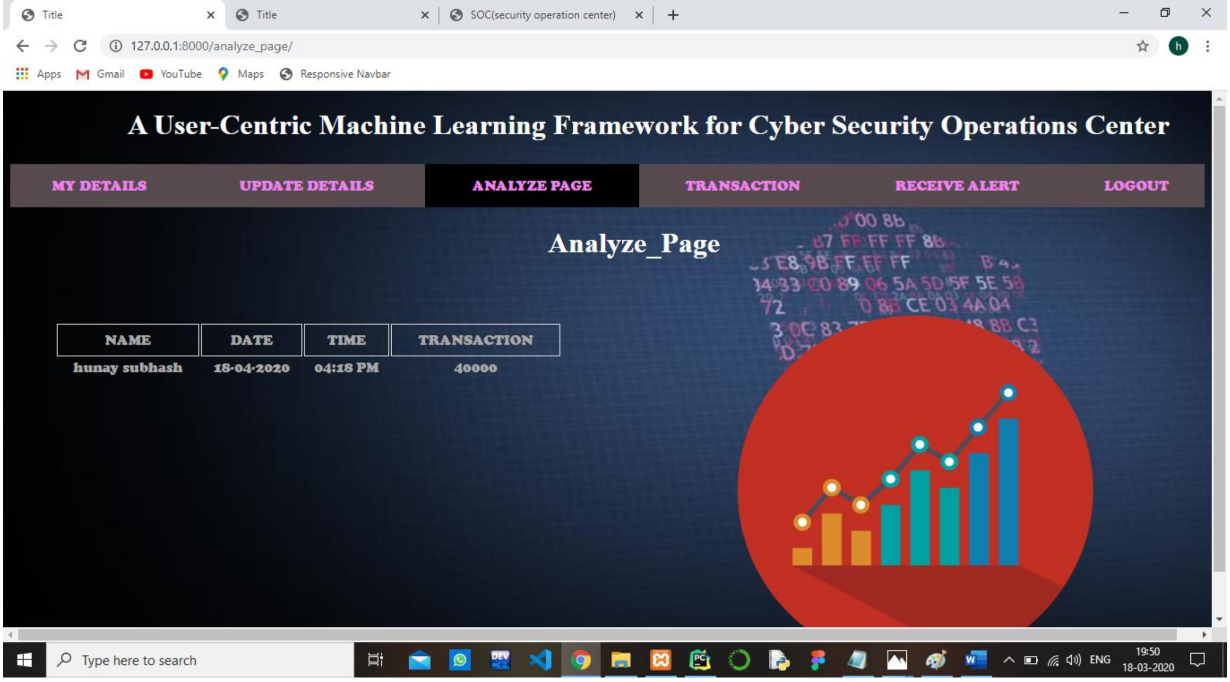
Admin Id	hunay11
Name	hunay subhash
Email	hunaysubhash97@gmail.cor
Password	hunay11
Phone Number	8074243934
Address	bhimavaram

Transaction With User Details Page



User Name :	hunay subhash
Aadhar Card No :	9876 7654 3456 4567
Address :	bhimavaram
Mobile No :	8074243934
Bank Name :	back of india
Account No :	678594567894
Branch Name :	back of india
Amount :	900000
IFSC Code :	bf12345680
MICR Code :	bhj9995755
Date :	18-04-2020
Time :	04:26 PM

User Analyze Page

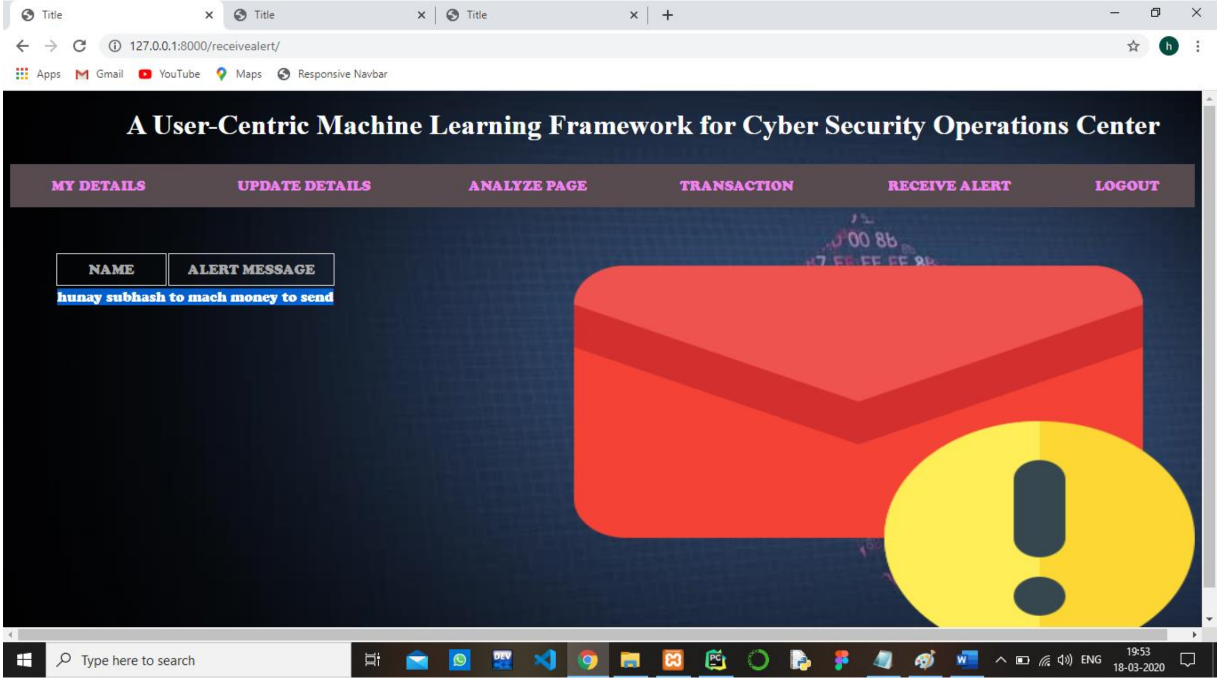


A User-Centric Machine Learning Framework for Cyber Security Operations Center

Analyze_Page

NAME	DATE	TIME	TRANSACTION
hunay subhash	18-04-2020	04:18 PM	40000

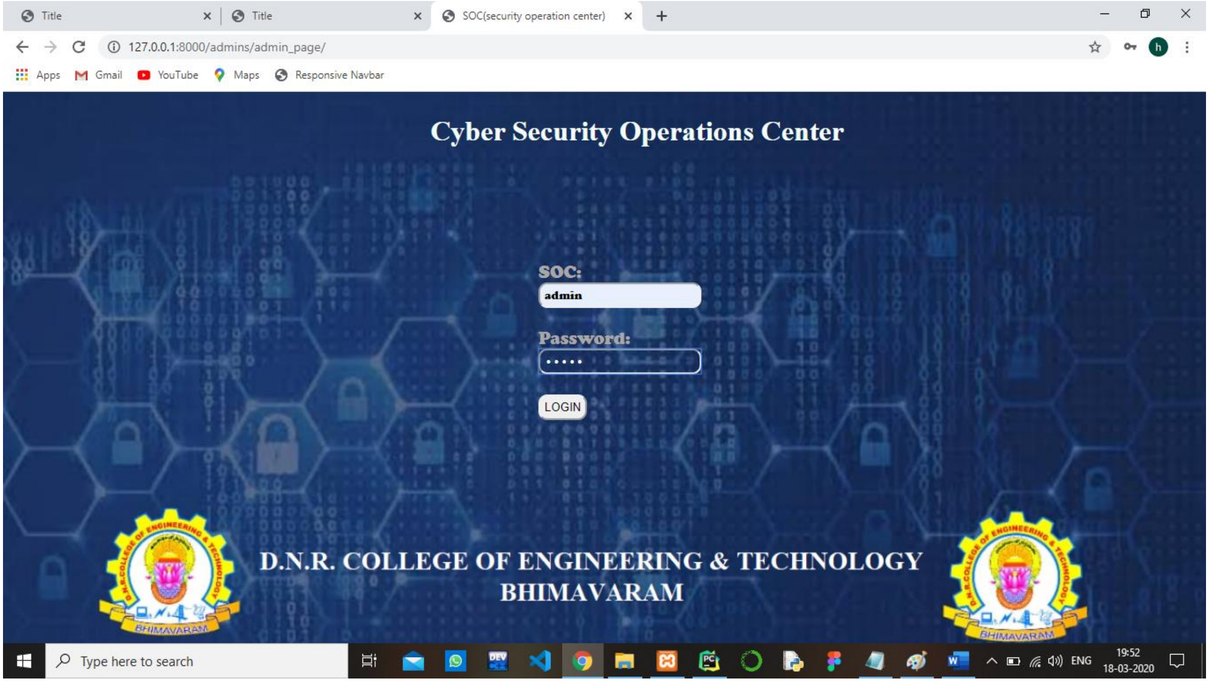
User Receive Alert Page



A User-Centric Machine Learning Framework for Cyber Security Operations Center

NAME	ALERT MESSAGE
hunay subhash	to mach money to send

Admin Login Page



127.0.0.1:8000/admins/admin_page/

Cyber Security Operations Center

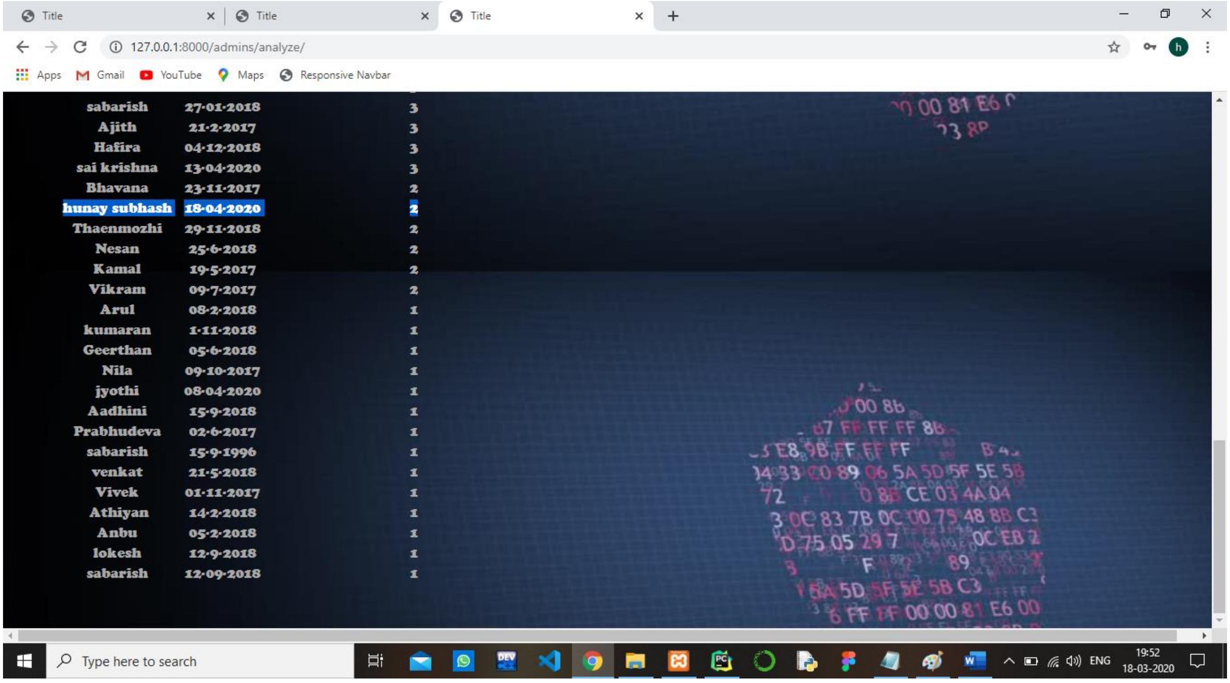
SOC: admin

Password: •••••

LOGIN

D.N.R. COLLEGE OF ENGINEERING & TECHNOLOGY
BHIMAVARAM

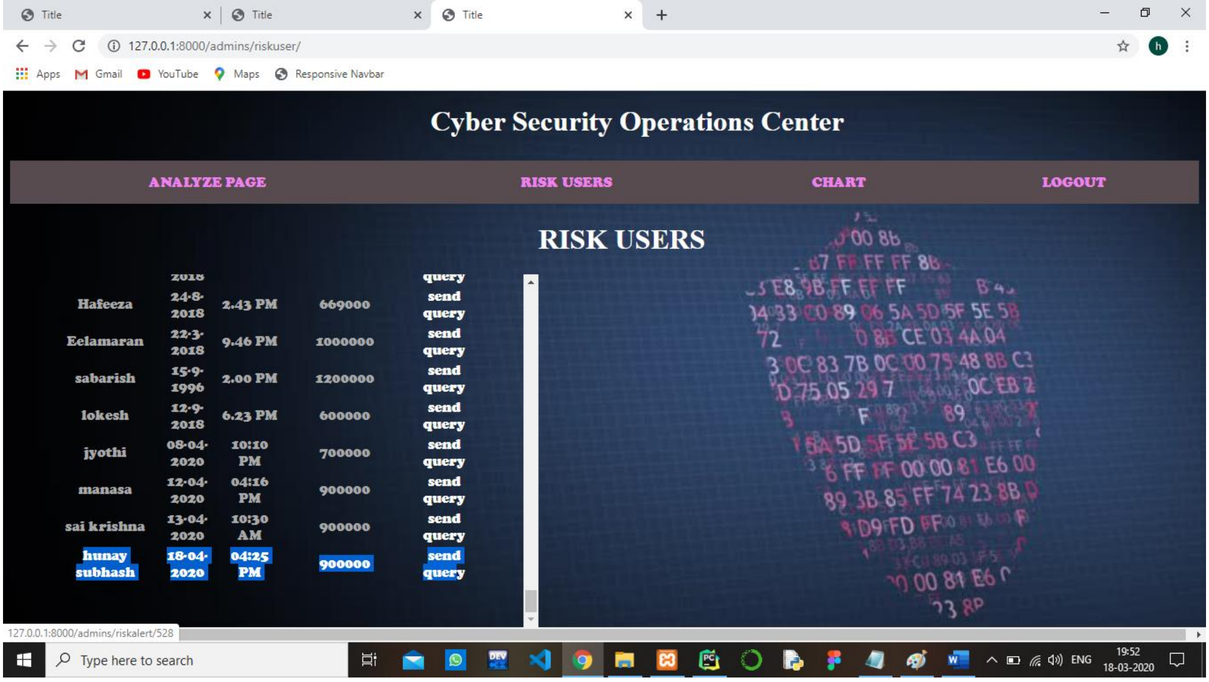
Admin Analyze Page



127.0.0.1:8000/admins/analyze/

sabarish	27-01-2018	3
Ajith	21-2-2017	3
Hafira	04-12-2018	3
sai krishna	13-04-2020	3
Bhavana	23-11-2017	2
hunay subhash	18-04-2020	2
Thaenmozhi	29-11-2018	2
Nesan	25-6-2018	2
Kamal	19-5-2017	2
Vikram	09-7-2017	2
Arul	08-2-2018	1
kumaran	1-11-2018	1
Geerthan	05-6-2018	1
Nila	09-10-2017	1
jyothi	08-04-2020	1
Aadhini	15-9-2018	1
Prabhudeva	02-6-2017	1
sabarish	15-9-1996	1
venkat	21-5-2018	1
Vivek	01-11-2017	1
Athiyan	14-2-2018	1
Anbu	05-2-2018	1
lokesh	12-9-2018	1
sabarish	12-09-2018	1

Admin Risk Users Page

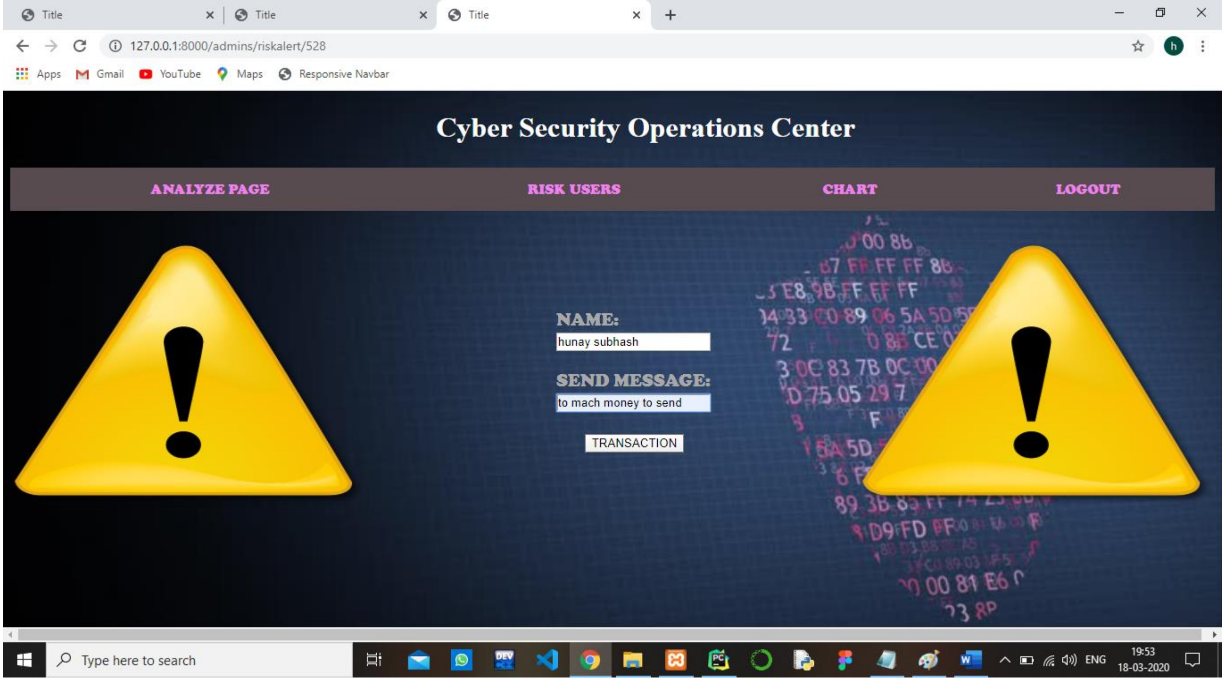


Cyber Security Operations Center

RISK USERS

	2018			query
Hafeeza	24-8-2018	2.43 PM	669000	send query
Eelamaran	22-3-2018	9.46 PM	1000000	send query
sabarish	15-9-1996	2.00 PM	1200000	send query
lokesh	12-9-2018	6.23 PM	600000	send query
jyothi	08-04-2020	10:10 PM	700000	send query
manasa	12-04-2020	04:16 PM	900000	send query
sai krishna	13-04-2020	10:30 AM	900000	send query
hunay subhash	18-04-2020	04:25 PM	900000	send query

Alert Message Sending Page

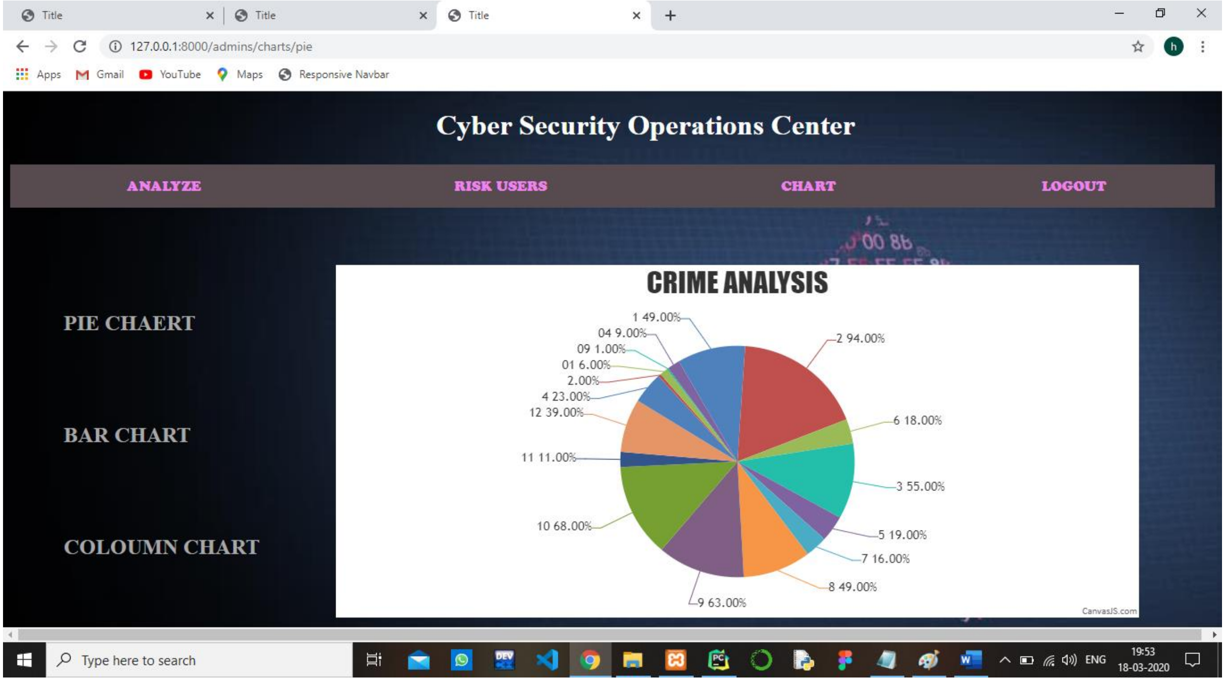


Cyber Security Operations Center

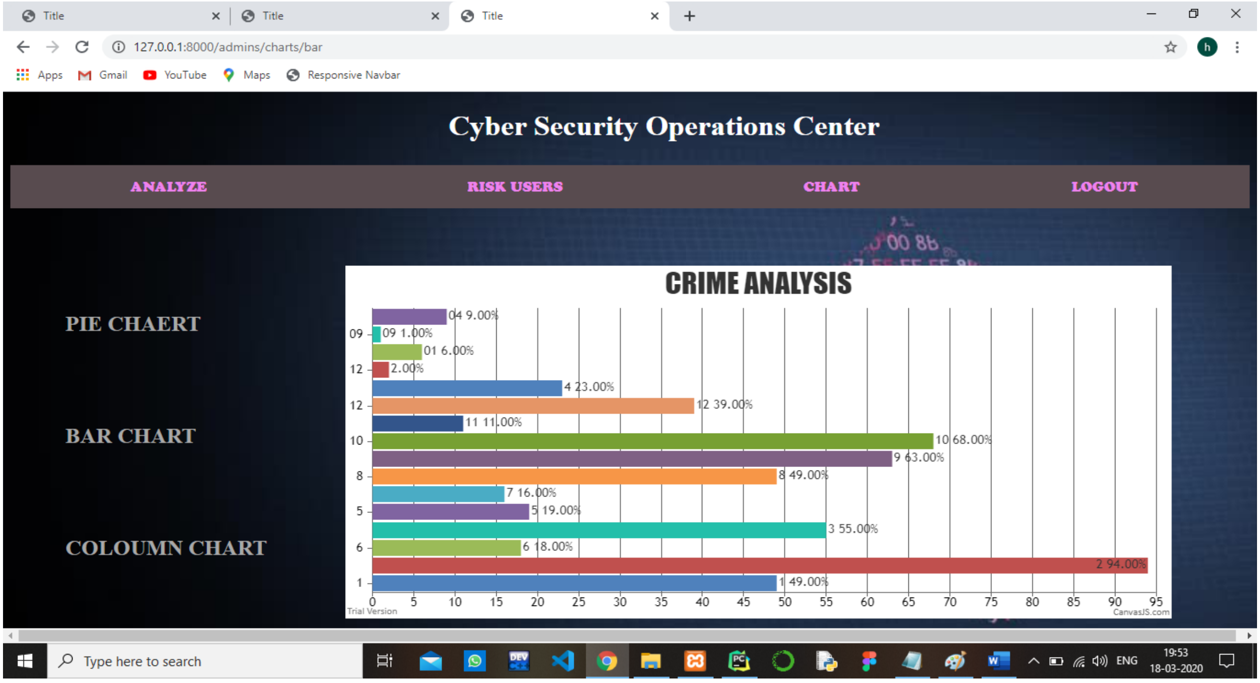
NAME: hunay subhash

SEND MESSAGE: to mach money to send

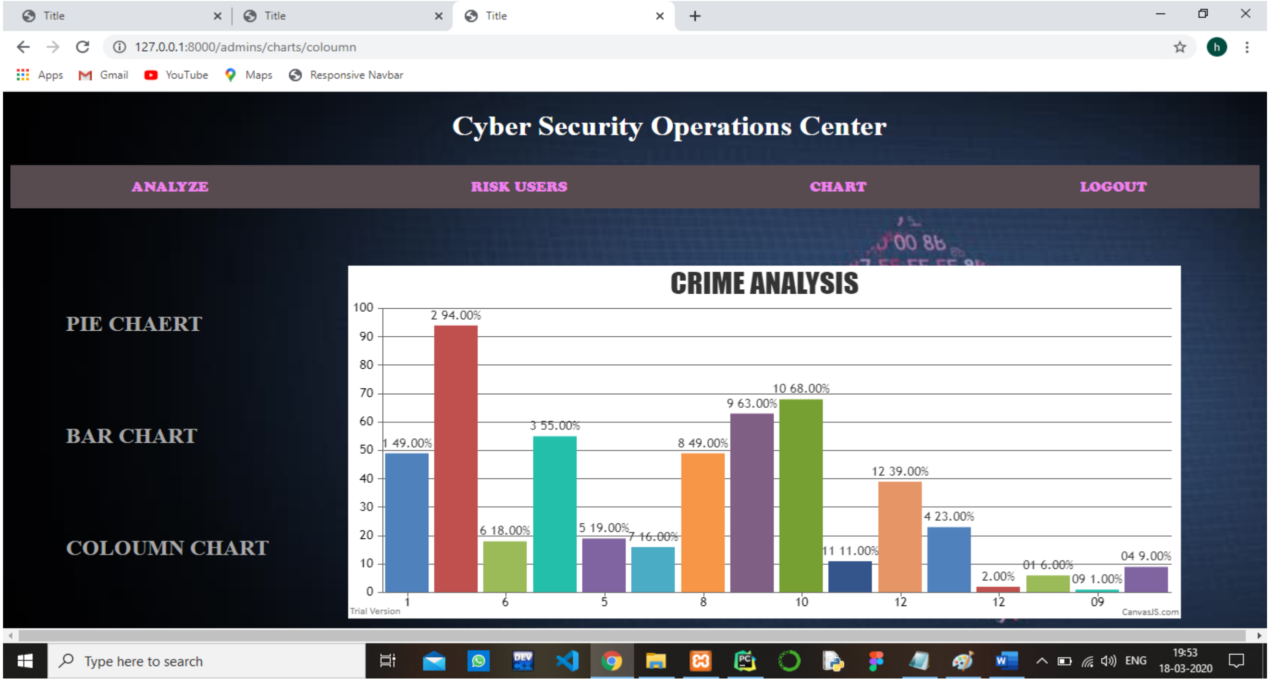
Graphical Analysis As Pie Chart



Graphical Analysis As Bar Chart



Graphical Analysis As Coloumn Chart



5. SYSTEM TESTING

5.1 Testing Concepts

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the

Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

5.2 Testing Strategies Applied

Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures : interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

5.3 TEST CASES

Test Cases For User Registration

Negative Test Case

Test Case 1: User Registration	Priority(H.L):High
Test Objective: to check the user registration wheatear register success or fail	
Test Description: In this Registration screen, when the user enters his/her details in the registration form and when he clicks the submit button then the database should respond if the user enters any invalid data and responds like please enter valid information, and if the data is correct the admin should store the information in the database and redirect him to the login page, or display an error.	
Requirement Verified: No	
Test Environment: System connected with the database.	
Actions	Expected Results
• when the user enters his/her details in the registration form and when he clicks the submit button, and the details are valid then it shows a message • When he enters a wrong password and then clicks submit button • When he enters a wrong e-mail and phone number and then clicks submit button.	• Registration fail • Enter valid data • Invalid User • Enter Valid email • Enter valid Phone number
Pass: no **Condition Pass**: No **Fail:** yes	
Problems/Issues: yes	
Notes: registration is fail	

Positive Test Case

Test Case 2: User Registration	Priority(H.L):High
Test Objective: to check the user registration wheatear register success or fail	
Test Description: In this Registration screen, when the user enters his/her details in the registration form and when he clicks the submit button then the database should respond if the user enters any invalid data and responds like please enter valid information, and if the data is correct the admin should store the information in the database and redirect him to the login page, or display an error.	
Requirement Verified: Yes	
Test Environment: System connected with the database.	
Actions	Expected Results
• when the user enters his/her details in the registration form and when he clicks the submit button, and the details are valid then it shows a message • When he enters a wrong password and then clicks submit button • When he enters a wrong e-mail and phone number and then clicks submit button.	Registration successful Enter valid data invalid user Enter Valid email Enter valid Phone number
Pass: Yes **Condition Pass**: Yes **Fail:** No	
Problems/Issues: No	
Notes: registration successfully completed	

Test Case For User Login

Negative Test Case

Test Case 1: User Login	Priority(H.L):High
Test Objective: has to check user login successful or fail	
Test Description: in this login page user enter his user name and password. After enter the user name password it has to compare with database values and validate the values. Once its match returns fail or success	
Requirement Verified: No	
Test Environment: System connected with the database.	
Actions	Expected Results
• Enter the user name and password • After the enter username and password verify with database • When he enters a wrong password and then clicks submit button	• Login fail • Enter valid data • Invalid user
Pass: No **Condition Pass**: No **Fail:** Yes	
Problems/Issues: Yes	
Notes: Login Fail	

Positive Test Case

Test Case 2: User Login	Priority(H.L):High
Test Objective: has to check user login successful or fail	
Test Description: in this login page user enter his user name and password. After enter the user name password it has to compare with database values and validate the values. Once its match returns fail or success	
Requirement Verified: Yes	
Test Environment: System connected with the database.	
Actions	Expected Results
• Enter the user name and password • After the enter username and password verify with database • When he enters a wrong password and then clicks submit button	• Login success • Enter valid data • Invalid user
Pass: Yes **Condition Pass**: Yes **Fail:** No	
Problems/Issues: No	
Notes: Login Success	

Test Case For Admin Login

Negative test case

Test Case 1: Admin Login	Priority(H.L):High
Test Objective: has to check admin login successful or fail	
Test Description: in this login page admin enter his admin name and password. After enter the admin name password it has to compare with database values and validate the values. Once its match returns fail or success	
Requirement Verified: No	
Test Environment: System connected with the database.	
Actions	Expected Results
• Enter the admin name and password • After the enter admin name and password verify with database • When he enters a wrong password and then clicks submit button	• Login fail • Enter valid data • Invalid admin
Pass: No **Condition Pass**: No **Fail:** Yes	
Problems/Issues: Yes	
Notes: Login fail	

Positive Test Case

Test Case 2: Admin Login	Priority(H.L):High
Test Objective: has to check admin login successful or fail	
Test Description: in this login page admin enter his admin name and password. After enter the admin name password it has to compare with database values and validate the values. Once its match returns fail or success	
Requirement Verified: Yes	
Test Environment: System connected with the database.	
Actions	Expected Results
• Enter the admin name and password • After the enter admin name and password verify with database • When he enters a wrong password and then clicks submit button	• Login Success • Enter valid data • Invalid admin
Pass: Yes **Condition Pass**: Yes **Fail:** No	
Problems/Issues: No	
Notes: Login Success	

6. CONCLUSION

We provide a user-centered computer learning system that affects large data from various security logs, awareness information, and inspector intelligence. This method provides complete configuration and solution for dangerous user detection for the Enterprise System Operating Center. Select machine learning methods in the SOC product environment, evaluate efficiency, IO, host and users to create user-centric features. . Even with simple mechanical learning algorithms, we prove that the learning system can understand more insights from the rankings with the most unbalanced and limited labels. More than 20% of the neurological model of modeling is 5 times that of the current rule-based system. To improve the detection precision situation, we will examine other learning methods to improve the data acquisition, daily model renewal, real time estimate, fully enhance and organizational risk detection and management. As for future work, let's examine other learning methods to improve detection accuracy

7. REFERENCES

[1] SANS Technology Institute. ³The 6 Categories of Critical Log Information´ 2013

[2] positive and unlabeled data´, Proceedings of the 18th international joint conference on Artificial intelligence, 2003

[3] A. L. Buczak and E. Guven. ³A survey of data mining and machine learning methods for cyber security intrusion detection´, IEEE Communications Surveys & Tutorials 18.2 (2015): 1153-1176.

[4] S. Choudhury and A. Bhowal. ³Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection´, Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015.

[5] N. Chand et al. ³A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection´, Advances in Computing, Communication, & Automation (ICACCA), 2016.

[6] K. Goeschel. ³Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis´, SoutheastCon, 2016.

[7] M. J. Kang and J. W. Kang. ³A novel intrusion detection method using deep neural network for in-vehicle network security´, Vehicular Technology Conference, 2016.