A

Major Project

On

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

(Submitted in partial fulfillment of the requirements for the award of Degree)

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

B. HEMANTH NAIDU(197R1A0505)

GANJI PALLAVI (197R1A0512)

P. VISHALA REDDY(197R1A0543)

Under the Guidance of

**Dr. K. SRUJAN RAJU**

( Professor)


**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**CMRTECHNICALCAMPUS**

**UGC AUTONOMOUS**

(Accredited by NAAC, NBA, Permanently Affiliated to JNTUH, Approved by AICTE, NewDelhi)

Recognized Under Section 2(f) & 12(B) of the UGCAct.1956, Kandlakoya (V), Medchal Road, Hyderabad-501401.

**2019-2023**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

# CERTIFICATE

This is to certify that the project entitled **"A USERCENTRIC MACHINE LEARNING FRAMEWORK FOR CYBER SECURITY OPERATIONS CENTER"**being submitted by **B. HEMANTH NAIDU (197R1A0505), GANJI PALLAVI (197R1A0512) & PATLOLLA VISHALA REDDY (197R1A0543)** in partial fulfillment of the requirements for the award of the degree of B.Tech in Computer Science and Engineering to the Jawaharlal Nehru Technological University Hyderabad, is a record of bonafide work carried out by them under our guidance and supervisionduring the year 2022-23.

The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

**Dr.K.Srujan Raju**
(Professor)
INTERNAL GUIDE

**Dr.A. Raji Reddy**
DIRECTOR

**Dr. K. Srujan Raju**
HOD

**EXTERNAL EXAMINER**

**Submitted for viva voice Examination held** _____

# ACKNOWLEDGEMENT

Apart from the efforts of us, the success of any project depends largely on the encouragement and guidelines of many others. We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project.

We take this opportunity to express my profound gratitude and deep regard to my guide **Dr.K.Srujan Raju,** Professor for his exemplary guidance, monitoring, and constant encouragement throughout the project work. The blessing, help, and advice given by him shall carry us a long way in the journey of life on which we are about to embark.

We also take this opportunity to express a deep sense of gratitude to the Project Review Committee (PRC) **Dr. Punyaban Patel, Ms. K. Shilpa, Dr. M . Subha Mastan Rao & J. Narasimharao** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K. Srujan Raju,** Head of the Department of Computer Science and Engineering, **Dr. Ashuthosh Saxena,** Dean R&D, and **Dr. D T V Dharmajee Rao,** Dean Academics for providing encouragement and support for completing this project successfully.

We are obliged to **Dr. A. Raji Reddy,** Director for being cooperative throughout the course of this project. We also express our sincere gratitude to Sri. **Ch. Gopal Reddy,** Chairmanfor providing excellent infrastructure and a nice atmosphere throughout the course of this project.

The guidance and support received from all the members of **CMR Technical Campus** contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

**B.HEMANTH NAIDU (197R1A0505)**
**GANJI PALLAVI (197R1A0512)**
**PATLOLLA VISHALA REDDY (197R1A0543)**

# ABSTRACT

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 thanthe 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/TABLES

# LIST OF SCREENSHOTS

## TABLE OF CONTENTS

# 1.INTRODUCTION

# 1. INTRODUCTION

By and by frameworks associated by the web, for example, the equipment, programming and information can be shielded from cyberattacks utilizing cybersecurity. Cybersecurity is a lot of advancements and procedures intended to secure PCs, networks, projects, and information from assaults and unapproved access, change, or obliteration. As dangers become increasingly refined the latest advancements, for example, Machine learning (ML) and profound learning (DL) are utilized in the cybersecurity network to use security capacities. These days, cybersecurity is an invigorating issue in the internet and it has been relying upon computerization of various application spaces, for example, accounts, industry, clinical, and numerous other significant zones [11]. To distinguish different network assaults, especially notrecently observed assaults, is a key issue to be settled desperately [1].This paper manages past work in machine learning (ML) and profound learning (DL) techniques for cybersecurity applications and a few utilizations of every strategy in cybersecurity tasks are depicted. The ML and DL techniques shrouded in this paper are pertinent to distinguish cybersecurity dangers, for example, programmers and predators, spyware, phishing, and network interruptionlocation in ML/DL. In this manner, incredible noticeable quality is set on an exhaustive portrayal of the ML/DL techniques, and references to original works for every MLand DL strategy are given [1]. What's more, examine the difficulties and chances of utilizing ML/DL for cybersecurity.

## 1.1 PROJECT SCOPE

It aims to provide user-centric engineer learning framework for the Internet Safety FunctionalCenter 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. Main scope of this project is to reduce the unwanted data for the dataset.

## 1.2 PROJECT PURPOSE

Machine learning is a viable approach to reduce the false positive rate and improve theproductivity of SOC analysts. provides complete configuration and solution

for dangerous user detection for the Enterprise System Operating Center.

## 1.3 PROJECT FEATURES

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. 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 decidewhether the user related to the alert is risky (a true positive) or not (false positive). However, SIEM typically generates a lot of the alerts, but with a very high false positive rate. The numberof 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 highseverity 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 findneedle 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 improvetheir efficiency.

# 2.LITERATURE SURVEY

# 2. LITERATURE SURVEY

## 2.1 DETECTING PORT SCAN ATTEMPTS WITH COMPARATIVE ANALYSIS OF DEEP LEARNING AND SUPPORT VECTOR MACHINE ALGORITHMS (DogukanAksu; M. Ali Aydin IEEE 2018).

Contrasted with the past, improvements in PC and correspondenceadvances have given broad anD propelled changes. The utilization of new advancements give extraordinary advantages to people, organizations, and governments, in any case, it messes some up against them. For instance, the protection of significant data, the security of put away information stages,accessibility of information and so on. Contingent upon these issues, digital fearbased oppression is one of the most significant issues in today's world. Digital fear, which made a ton of issues people and foundations, has arrived at a level that could undermine open and national security by different gatherings, for example, criminal associations, proficient people and digital activists. In this manner, Intrusion Detection Systems (IDS) have been created to keep away fromdigital assaults. In this examination, profound learning and bolster vector machine (SVM) calculations were utilized to identify port sweep endeavors dependent on the new CICIDS2017 dataset and 97.80%, 69.79% precision rateswere accomplished separately.

## 2.2 DETECTING CYBER-ATTACKS USING A CRPS-based MONITORING APPROACH (Fouzi Harrou; Benamar Bouyeddou; Ying Sun; Benamar Kadri IEEE 2018).

Digital assaults can genuinely influence the security of PCs and system frameworks. In this manner, building up a productive oddity location component is significant for data insurance and digital security. To precisely identify TCP SYN flood assaults, two factual plans dependent on the nonstop positioned likelihood score (CRPS) metric have been planned in this paper. In particular, byincorporating the CRPS measure with two ordinary graphs, Shewhart and the exponentially weighted moving normal (EWMA) diagrams, novel abnormality discovesystems were created: CRPS-Shewhart and CRPS EWMA. The effectiveness of the proposed techniques has been confirmed utilizing the 1999 DARPA interruption identification assessment datasets.

## 2.3 A TAXONOMY OF MALICIOUS TRAFFIC FOR INTRUSION DETECTION SYSTEMS (HananHindy; Alike Hodo; Ethan Bayne; Amar Steam;Robert Atkinson; Xavier Bellekens IEEE 2018).

With the expanding number of system dangers, it is fundamental to have any information on existing and new system dangers to configuration better interruption identification frameworks. In this paper we propose a scientific classification for ordering system assaults in a predictable manner, enabling security analysts to concentrate their endeavors on making exact interruption discovery frameworks and focused on datasets.

## 2.4 PARAMETER-INVARIANT MONITOR DESIGN FOR CYBER PHYSICALSYSTEMS (James Weimer; RadoslavIvanov; Sanjian Chen; Alexander Roederer; Oleg Sokolsky; Insup Lee IEEE 2018).

The tight collaboration between data innovation and the physical world intrinsic in digital-physical frameworks (CPS) can challenge customary methodologies for observing wellbeing and security. Information gathered for vigorous CPS checking is frequently meager and may need rich preparing information depicting basic occasions/assaults. Besides, CPS regularly works in different conditions that can have critical entomb/intraframework inconstancy. Besides, CPS screens that are not hearty to information sparsity andbury/intraframework changeability may bring about conflicting execution and may not be trusted for observing wellbeing and security. Towards beating these difficulties, this paper presents ongoing work on the structure of parameter- invariant (PAIN) screens for CPS. Agony screens are planned with the end goal that obscure occasions and framework inconstancy negligibly influence thescreen execution. This work portrays how PAIN structures can accomplish a consistent bogus caution rate (CFAR) within the sight of information sparsity and intra/entomb system variance in genuine CPS. To show the plan of PAIN screens for security checking in CPS with various kinds of elements, we think about frameworks with organized elements, direct time-invariant elements, and half and half elements that are examined through contextual investigations for building actuator deficiency identification, feast location in type I diabetes, and identifying hypoxia brought about by pneumonic shunts in babies. In all applications, the PAIN screen is appeared to have (fundamentally) less differencein

checking execution and (frequently) beats other contending approaches in the writing. At long last, an underlyinguse of PAIN observing for CPS security is displayed alongside difficulties and research headings for future security checking arrangement.

# 3.SYSTEM ANALYSIS

# 3. SYSTEM ANALYSIS

System Analysis is the important phase in the system development process. The System is studied to the minute details and analyzed. The system analyst plays an important of an interrogatorand dwells deep into the working of the present system. In analysis, a detailed study of these operations performed by the system and their relationships within and outside the system is done.Akey question considered here is, “what must be done to solve the problem?” The system is viewed as a whole and the inputs to the system are identified. Once analysis is completed the analyst has a firm understanding of what is to be done.

## 3.1 PROBLEM DEFINATION

This presents a study on real-time face mask detection using OpenCV and deep learning techniques and based on the results obtained, it is a noteworthy method for easy detection of face mask. An organization can monitor employees and their safety. And Medical officials can monitorthe society to make health policies.

## 3.2 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 trafficdata, 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 thatthe 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.

### 3.2.1 DISADVANTAGES :

1. Firewalls can be difficult to configure correctly.
2. Incorrectly configured firewalls may block users from performingactions on the Internet, until the firewall configured correctly.
3. Makes the system slower than before.
4. Nee d to keep updating the new software to keep security up to date.
5. Could be costly for the average user.
6. The user is the only constant.

## 3.3 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 areaffected by security threats because of their complexity and cyber-security connectivity. TheseCPSs face security breaches when people, processes, technology, or othercomponents are being attacked or risk management systems are missing, inadequate, or fail inany way. The attackerstarget confidential data.

for the dataset.

### 3.3.1 ADVANTAGES

1. Protection against data from theft.
2. Protects the computer from being hacked.
3. Minimizes computer freezing and crashes.
4. Gives privacy to users
5. Securing the user-aware network edge
6. Securing mobile users' communications .
7. Managing user-centric security.

## 3.4 FEASIBILITY STUDY

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

***FEASIBILITY**

***TECHNICAL FEASIBILITY**

***SOCIAL FEASIBILITY**

### 3.4.1 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 withinthe budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

### 3.4.2 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 availabletechnical resources. This will lead to high demands on the available technical resources. This willlead 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.

### 3.4.3 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 userssolely 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.

## 3.5 SYSTEM REQUIRMENTS AND SPECIFICATION

## REQUIREMENT ANALYSIS

The project involved analyzing the design of few applications so as to make the applicationmore users friendly. To do so, it was really important to keep the navigations from one screen to the other well ordered and at the same time reducing the amount of typing the user needs to do. In order to make the application more accessible, the browser version had to be chosen so that it is compatible with most of the Browsers.

### 3.5.1 FUNCTIONAL REQUIREMENTS

Functional requirement should include function performed by a specific screen outline work-flows performed by the system and other business or compliance requirement the system must meet. Functional requirements specify which output file should be produced from the given file they describe the relationship between the input and output of the system, for each functional requirement a detailed description of all data inputs and their source and the range of valid inputs must be specified. The

functional specification describes what the system must do, how the systemdoes it is described in the design specification. If a user requirement specification was written, all requirements outlined in the user requirements specifications should be addressed in the functionalrequirements.

### 3.5.2 NON-FUNCTIONAL REQUIREMENTS

Describe user-visible aspects of the system that are not directly related with the functional behavior of the system. Non-Functional requirements include quantitative constraints, such as response time (i.e. how fast the system reacts to user commands.) or accuracy (.e. how precise arethe systems numerical answers.

### 3.5.3 INPUT DESIGN

The input design is the link between the information system and the user. It comprises thedeveloping specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the

privacy Input Design considered the following things:

* What data should be given as input?
* How the data should be arranged or coded?
* The dialog to guide the operating personnel in providing input.
* Methods for preparing input validations and steps to follow when error occur.

### 3.5.4 OBJECTIVES

Input Design is the process of converting a user-oriented description of the input into a computerbased system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. Thedata entry screen is designed in such a way that all the data manipulates can be performed. Italso provides record viewing facilities.

The data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

### 3.5.5 OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to othersystem through outputs. In output design it is determined how the information is to be displaced forimmediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

- Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
- Select methods for presenting information.
- Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the followingobjectives.

- Convey information about past activities, current status or projections of the  Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

## 3.6 HARDWARE REQUIREMENTS AND SOFTWARE REQUIREMENTS

### 3.6.1 HARDWARE REQUIREMENTS

* Hard Disk : 40 GB.
* Ram : 512 Mb.

### 3.6.2 SOFTWARE REQUIREMENTS:

*Operating system: Windows 10.

*Coding Language: Python.

* Front-End: Python.

*Designing: Html, CSS, JavaScript.

*Data Base: MySQL.

# 4.ARCHITECTURE

# 4.ARCHITECTURE

## 4.1 PROJECT ARCHITECTURE

The System architecture represents the design process that identifies the subsystems which constitute the framework and system for control and communication. Its intention is to establish the overallstructure and interactions of a software system.

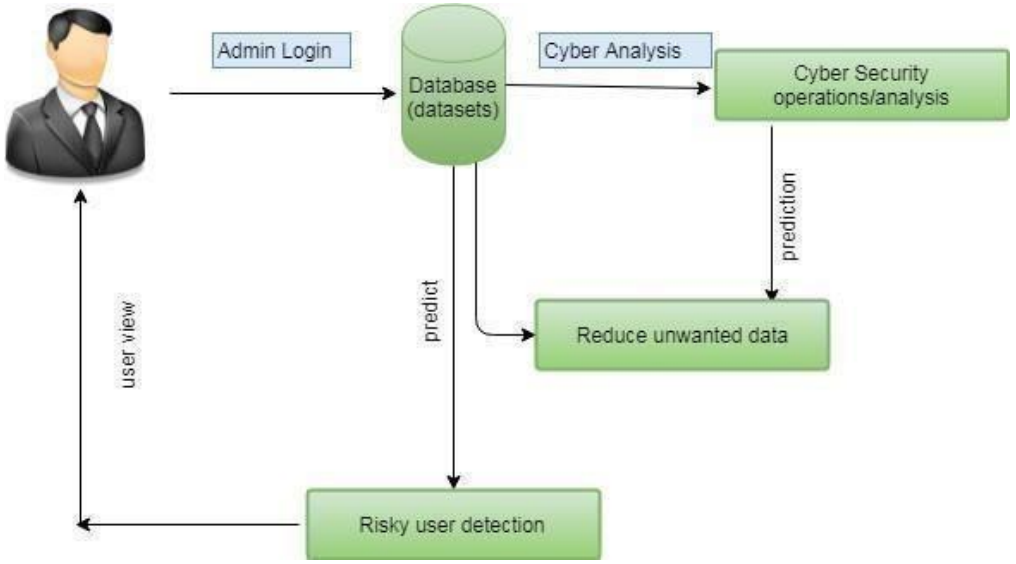



Figure 4.1 Project Architecture

## 4.2 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 cyberattacks 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 couldbe 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 metricbased 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 simplydeleting 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 allkinds 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. For example, if you decide toimport 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 metricbased on an attribute, To create an attribute based on a metric, To define the geo role for an attribute, To create anattribute with additional time information, To replace a dataset object in the dashboard.

## 4.3 UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for businessmodeling and other nonsoftware systems.

Relationships depict a connection between several things, such as structural, behavioral, or grouping things in the unified modeling language. Since it is termed as a link, it demonstrates how things are interrelated to each other at the time of system execution. It constitutes four types of relationships, i.e., **dependency, association, generalization,** and **realization.** Unified Modeling Language (UML) Models represent systems at different levels of detail. Some models describe a system from a higher, more abstract level, while other models provide greater detail.

You create and manage models using modeling projects in the Project Explorer view. The contents of a modeling project are organized into three types of logical folders: diagrams, models, and profiles. This structure displays the logical containment of the UML model elements, regardless of where they are stored physically. The models in a modeling project are displayed under the Models folder, or node. These nodes are not the physical model files, which have the .emx as a file name extension, but are the root model elements of the models. Similarly, the corresponding diagrams and profiles are displayed under the Diagrams folder and Profiles folder respectively

You can use modeling diagrams to capture system use cases in a use-case model during the requirements gathering phase, you define the application domain in an analysis model during the system analysis phase, and you refine the application model in a design model during the detailed design phase.

## GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop andexchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.

## 4.3.1 USE CASE DIAGRAM

Use case diagrams are considered for high level requirement analysis of a system. So when the requirements of a system are analyzed the functionalities are captured in use cases.Sowe can say that uses cases are nothing but the system functionalities written in an organized manner. Now the second things which are relevant to the use cases are the actors. Actors can be defined as something that interacts with the system.

The actors can be human user, some internal applications or may be some external applications.So in a brief when we are planning to draw an use case diagram we should have the followingitems identified.

*Functionalities to be represented as an use case

*Actors

* Relationships among the use cases and actors.

a. user

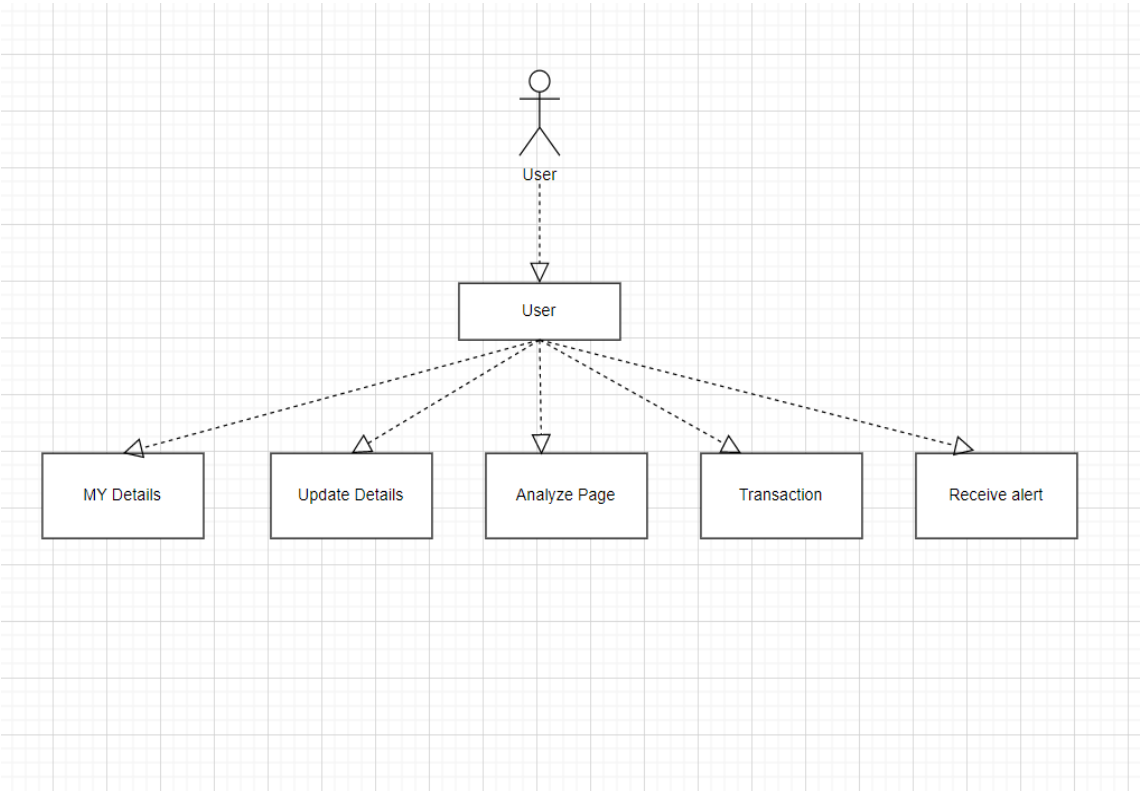



Figure 4.3.1: Use case diagram of user

b.admin

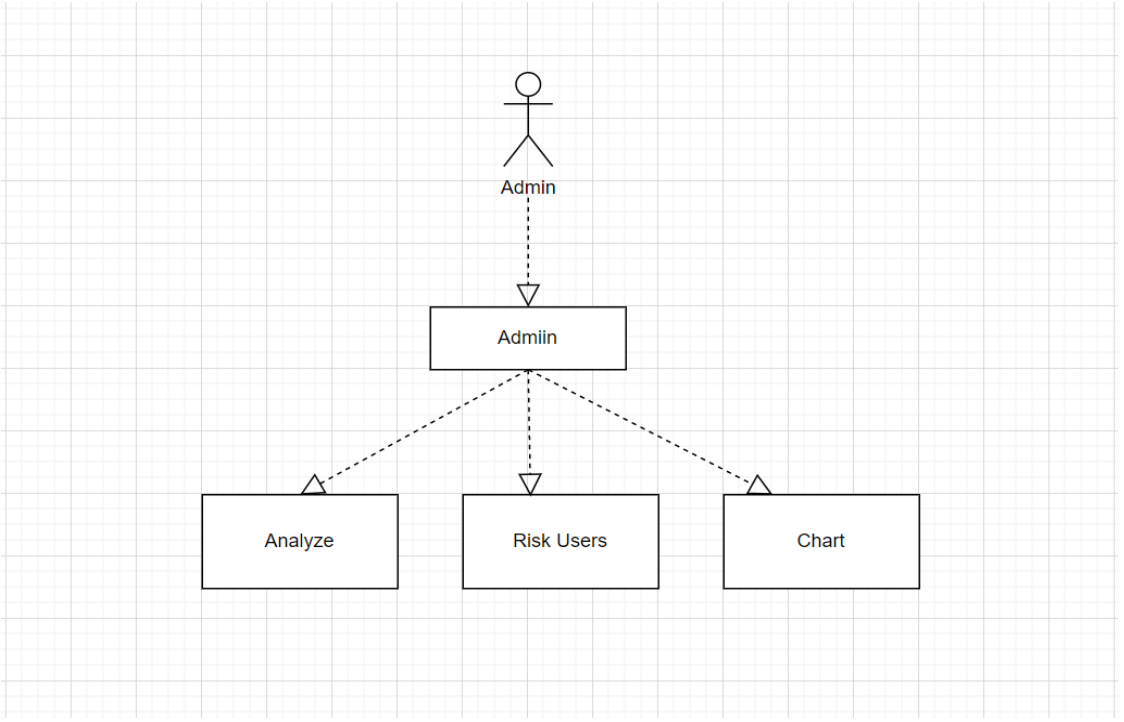



Figure 4.3.1: Use case diagram of admin.

### 4.3.2 SEQUENCE DIAGRAM

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a constructof a Message Sequence Chart. A sequence diagram shows, as parallel vertical lines ("lifelines"), different processes or objects that live simultaneously, and, as horizontal arrows, the messagesexchanged between them, in the order in which they occur. This allows the specification of simple runtime scenarios in a graphical manner.

a.user

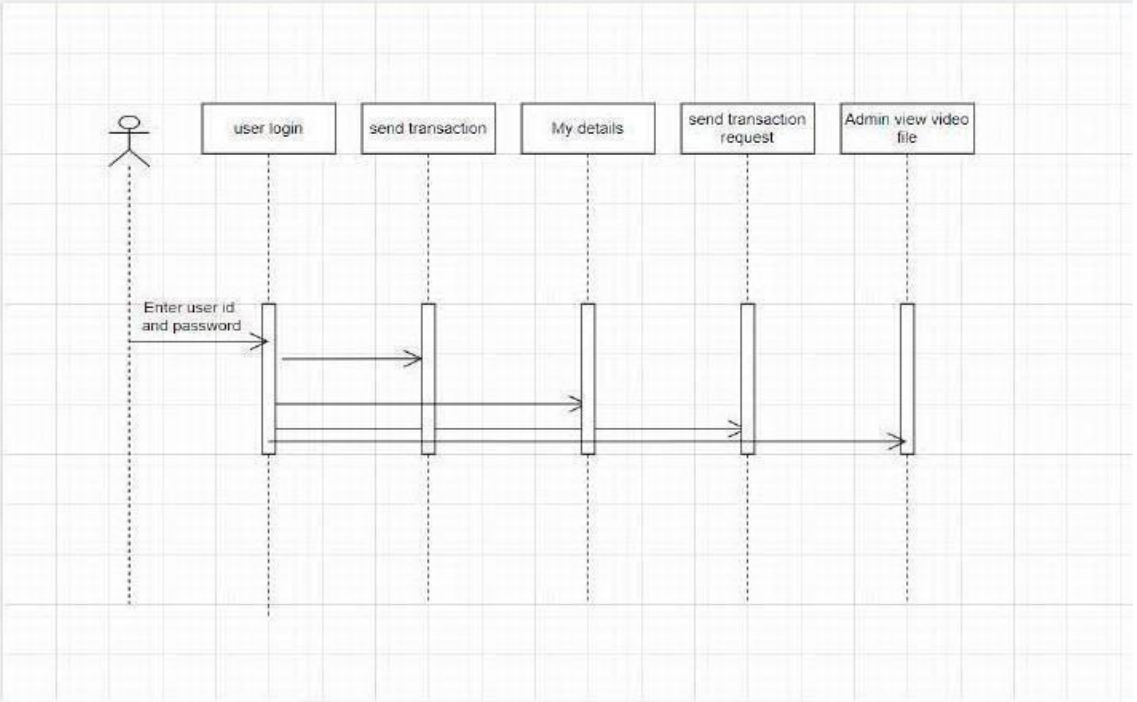



Figure 4.3.2: Sequence diagram of user

b.admin

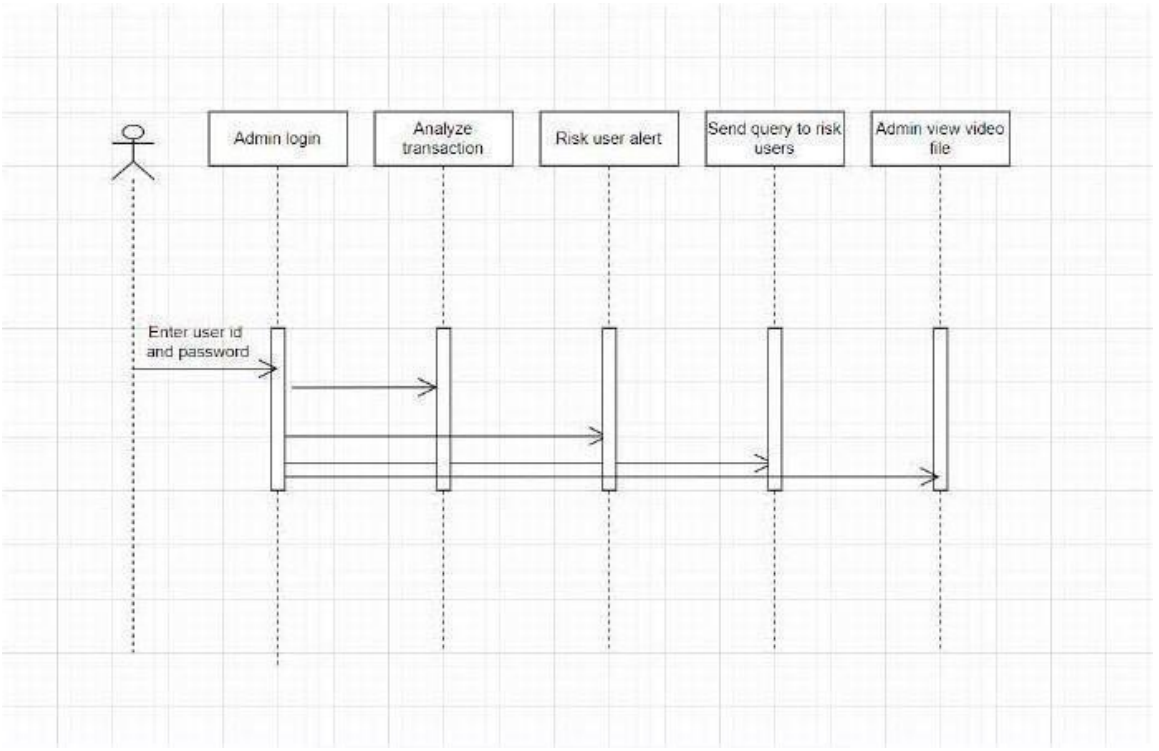



Figure 4.3.2: Sequence diagram of user.

### 4.3.3 ACTIVITY DIAGRAM

Activity diagrams are graphical representations of Workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by- step workflows of components in a system. An activity diagram shows the overall flow ofcontrol.

a .user

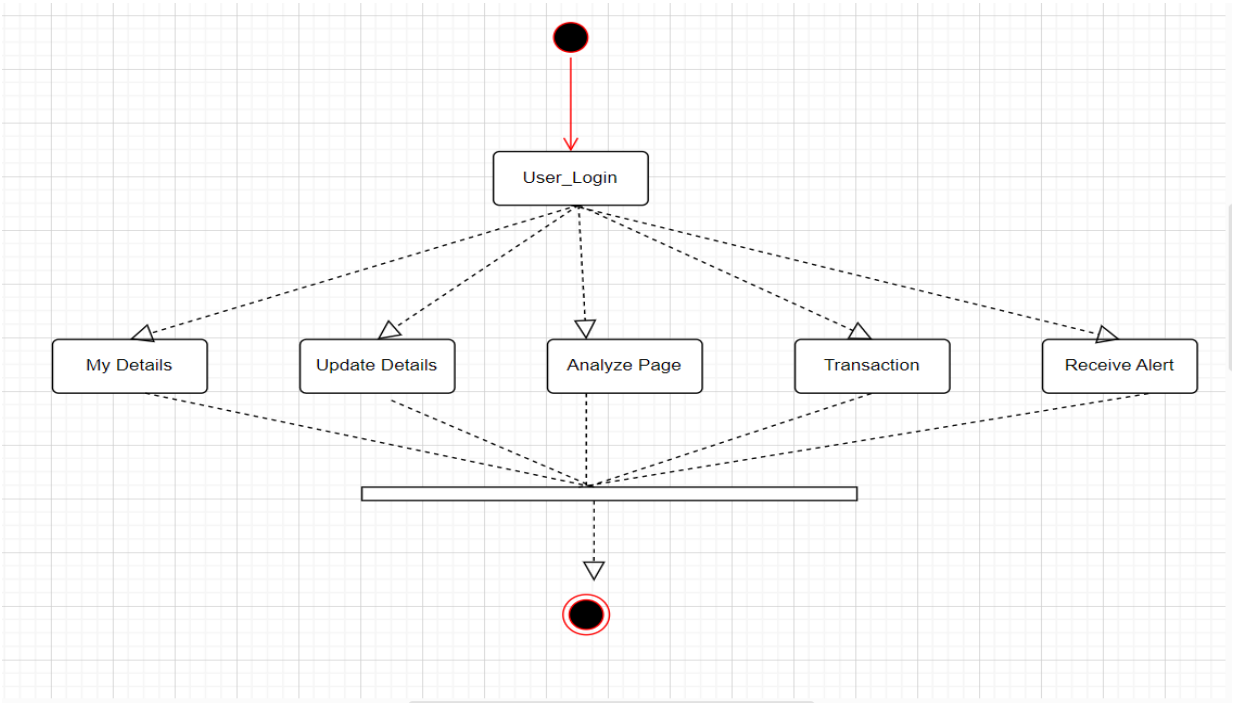



Figure 4.3.3: Activity diagram of user

b. admin

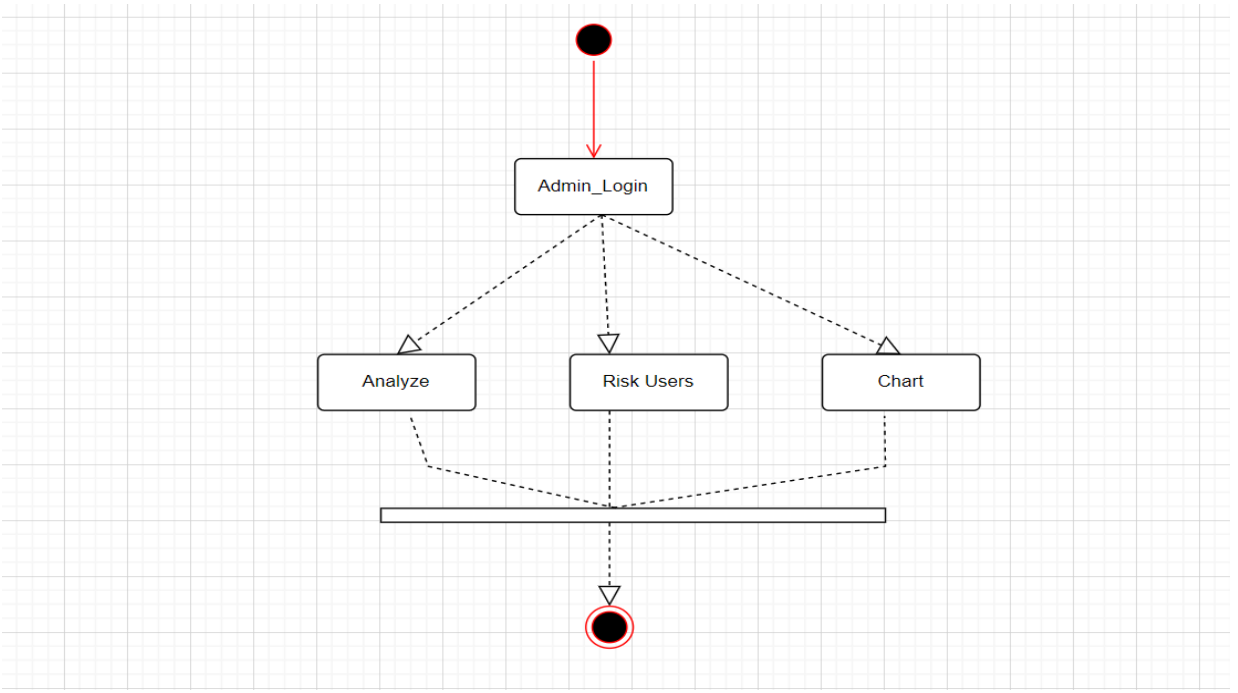



Figure 4.3.3: Activity diagram of admin.

# 5.IMPLEMENTATION

# 5. IMPLEMENTATION

## 5.1 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 valueof 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 doneby 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.

## 5.2 TECHNOLOGY DESCRIPTION

### Introduction of Python:

Python is a general-purpose interpreted, interactive, object-oriented, and high-level programming language. An interpreted language, Python has a design philosophy that emphasizes code readability (notably using whitespace indentation to delimit code blocks rather than curly brackets or keywords), and a syntax that allows programmers to express concepts in fewer lines of code than might be used in languages such as C++or Java. It provides constructs that enable clear programming on both small and large scales. Python interpreters are available for many operating systems. C, Python, the reference implementation of Python, is open source software and has a community-based development model, as do nearly all of its variant implementations. C, Python is managed by the non- profit Python Software Foundation. Python features a dynamic type system and automatic memory management. It supports multiple programming paradigms, including object- oriented, imperative, functional and procedural, and has a large and comprehensive standard library.

### Python Install

Many PCs and Macs will have python already installed.
To check if you have python installed on a Windows PC, search in the start bar for Python or run the following on the Command Line (cmd.exe):
C:\Users\Your Name>python --version
To check if you have python installed on a Linux or Mac, then on linux open the command line or on Mac open the Terminal and type:
python –version

If you find that you do not have python installed on your computer, then you can download itfor free from the following website: https://www.python.org/.

# Virtual Environments and Packages

## Introduction

Python applications will often use packages and modules that don't come as part of the standard library. Applications will sometimes need a specific version of a library, because the application may require that a particular bug has been fixed or the application may be written using an obsolete version of the library's interface.

This means it may not be possible for one Python installation to meet the requirements of every application. If application A needs version 1.0 of a particular module but applicationB needs version 2.0, then the requirements are in conflict and installing either version 1.0or 2.0will leave one application unable to run.

The solution for this problem is to create a virtual environment, a self-contained directory tree that contains a Python installation for a particular version of Python, plus a few additional packages.

Different applications can then use different virtual environments. To resolve the earlier example of conflicting requirements, application A can have its own virtual environment with version 1.0 installed while application B has another virtual environmentwith version 2.0. If application B requires a library be upgraded to version 3.0, this will not affect application A's environment.

### Creating Virtual Environments

The module used to create and manage virtual environments is called venv. venv will usually install the most recent version of Python that you have available. If you have multiple versions of Python on your system, you can select a specific Python version by running python3 or whichever version you want.

To create a virtual environment, decide upon a directory where you want to place it, and run the venv module as a script with the directory path:

python3 -m venv tutorial-env

This will create the tutorial-env directory if it doesn't exist, and also create directories inside it containing a copy of the Python interpreter, the standard library, and various supporting files.A common directory location for a virtual environment is .venv. This name keeps the directorytypically hidden in your shell and thus out of the way while giving it a name that explains whythe directory exists. It also prevents clashing with .env environment variable definition files that some tooling supports.

Once you've created a virtual environment, you may activate it.On Windows, run:

tutorial-env\Scripts\activate.batOn Unix or MacOS, run:

source tutorial-env/bin/activate

(This script is written for the bash shell. If you use the csh or fish shells, there are alternateactivate.csh and activate.fish scripts you should use instead.)

Activating the virtual environment will change your shell's prompt to show what virtual environment you're using, and modify the environment so that running python will get you that particular version and installation of Python. For example:

$ source ~/envs/tutorial-env/bin/activate(tutorial-env) $ python

Python 3.5.1 (default, May 6 2016, 10:59:36)

...

>>> import sys

>>>sys.path

['', '/usr/local/lib/python35.zip', ..., '~/envs/tutorial-env/lib/python3.5/site-packages']

>>>

**Managing Packages with pip**

You can install, upgrade, and remove packages using a program called pip. By default pip willinstall packages from the Python Package Index, <https://pypi.org>. You can browse the Python Package Index by going to it in your web browser, or you can use pip's limited searchfeature:

(tutorial-env) $ pip search astronomy

skyfield - Elegant astronomy for Python

gary - Galactic astronomy and gravitational dynamics.

novas - The United States Naval Observatory NOVAS astronomy libraryastroobs - Provides astronomy ephemeris to plan telescope observations

PyAstronomy - A collection of astronomy related tools for Python.

...

pip has a number of subcommands: “search”, “install”, “uninstall”, “freeze”, etc. (Consult theInstalling Python Modules guide for complete documentation for pip.)

You can install the latest version of a package by specifying a package’s name:(tutorial-env) $ pip install novas

Collecting novas

Downloading novas-3.1.1.3.tar.gz (136kB)Installing collected packages: novas

Running setup.py install for novas Successfully installed novas-3.1.1.3

You can also install a specific version of a package by giving the package name followed by

== and the version number:

(tutorial-env) $ pip install requests==2.6.0Collecting requests==2.6.0

Using cached requests-2.6.0-py2.py3-none-any.whlInstalling collected packages: requests

Successfully installed requests-2.6.0

If you re-run this command, pip will notice that the requested version is already installed and do nothing. You can supply a different version number to get that version, or you can run pip install --upgrade to upgrade the package to the latest version:

(tutorial-env) $ pip install --upgrade requestsCollecting requests

Installing collected packages: requests Found existing installation: requests 2.6.0

Uninstalling requests-2.6.0:

Successfully uninstalled requests-2.6.0Successfully installed requests-2.7.0

pip uninstall followed by one or more package names will remove the packages from thevirtual environment.

**pip show will display information about a particular package:**

(tutorial-env) $ pip show requests
---
Metadata-Version: 2.0Name: requests Version: 2.7.0
Summary: Python HTTP for Humans. Home-page: http://python-requests.orgAuthor: Kenneth Reitz
Author-email: me@kennethreitz.comLicense: Apache 2.0
Location: /Users/akuchling/envs/tutorial-env/lib/python3.4/site-packagesRequires:
pip list will display all of the packages installed in the virtual environment:

(tutorial-env) $ pip listnovas (3.1.1.3)
numpy (1.9.2)
pip (7.0.3)
requests (2.7.0)
setuptools (16.0)
pip freeze will produce a similar list of the installed packages, but the output uses the formatthat pip install expects. A common convention is to put this list in a requirements.txt file:

(tutorial-env) $ pip freeze > requirements.txt(tutorial-env) $ cat requirements.txt
novas==3.1.1.3
numpy==1.9.2 requests==2.7.0

The requirements.txt can then be committed to version control and shipped as part of anapplication. Users can then install all the necessary packages with install -r:

```
(tutorial-env) $ pip install -r requirements.txt
Collecting novas==3.1.1.3 (from -r requirements.txt (line 1))
...
Collecting numpy==1.9.2 (from -r requirements.txt (line 2))
...
Collecting requests==2.7.0 (from -r requirements.txt (line 3))
...
Installing collected packages: novas, numpy, requestsRunning setup.py install for novas
Successfully installed novas-3.1.1.3 numpy-1.9.2 requests-2.7.0
```

pip has many more options. Consult the Installing Python Modules guide for complete documentation for pip. When you've written a package and want to make it available on the Python Package Index, consult the Distributing Python Modules guide.

## Introduction to Artificial Intelligence

"The science and engineering of making intelligent machines, especially intelligent computer programs". -John McCarthy-

Artificial Intelligence is an approach to make a computer, a robot, or a product to think how smart human think. AI is a study of how human brain think, learn, decide and work, when it tries to solve problems. And finally this study outputs intelligent software systems.The aim ofAI is to improve computer functions which are related to human knowledge, for example, reasoning, learning, and problem-solving.

The intelligence is intangible. It is composed of

* Reasoning
* Learning
* Problem Solving
* Perception
* Linguistic Intelligence

The objectives of AI research are reasoning, knowledge representation, planning, learning, natural language processing, realization, and ability to move and manipulate objects. There arelong-term goals in the general intelligence sector.

Approaches include statistical methods, computational intelligence, and traditional coding AI.During the AI research related to search and mathematical optimization, artificial neural networks and methods based on statistics, probability, and economics, we use many tools. Computer science attracts AI in the field of science, mathematics, psychology, linguistics, philosophy and so on.

Major Goals

* Knowledge reasoning
* Planning
* Machine Learning
* Natural Language Processing
* Computer Vision.

## Machine Learning

## Introduction

Machine learning is a subfield of artificial intelligence (AI). The goal of machine learning generally is to understand the structure of data and fit that data into models that can be understood and utilized by people.

Although machine learning is a field within computer science, it differs from traditional computational approaches. In traditional computing, algorithms are sets of explicitly programmed instructions used by computers to calculate or problem solve. Machine learning algorithms instead allow for computers to train on data inputs and use statistical analysis in order to output values that fall within a specific range. Because of this, machine learning facilitates computers in building models from sample data in order to automate decision- making processes based on data inputs.

Any technology user today has benefitted from machine learning. Facial recognition technology allows social media platforms to help users tag and share photos of friends. Opticalcharacter recognition (OCR) technology converts images of text into movable type. Recommendation engines, powered by machine learning, suggest what movies or television shows to watch next based on user preferences. Self-driving cars that rely on machine learningto navigate may soon be available to consumers.

Machine learning is a continuously developing field. Because of this, there are some

considerations to keep in mind as you work with machine learning methodologies, or analyze the impact of machine learning processes.

In this tutorial, we'll look into the common machine learning methods of supervised and unsupervised learning, and common algorithmic approaches in machine learning, including thek-nearest neighbor algorithm, decision tree learning, and deep learning. We'll explore which programming languages are most used in machine learning, providing you with some of the positive and negative attributes of each. Additionally, we'll discuss biases that are perpetuatedby machine learning algorithms, and consider what can be kept in mind to prevent these biaseswhen building algorithms.

## Machine Learning Methods

In machine learning, tasks are generally classified into broad categories. These categories are based on how learning is received or how feedback on the learning is given to the system developed.

Two of the most widely adopted machine learning methods are supervised learning which trains algorithms based on example input and output data that is labeled by humans, and unsupervised learning which provides the algorithm with no labeled data in order to allow it to find structure within its input data. Let's explore these methods in more detail.

## Supervised Learning

In supervised learning, the computer is provided with example inputs that are labeled with theirdesired outputs. The purpose of this method is for the algorithm to be able to "learn" by comparing its actual output with the "taught" outputs to find errors, and modify the model accordingly. Supervised learning therefore uses patterns to predict label values on additional unlabeled data.

For example, with supervised learning, an algorithm may be fed data with images of sharks labeled as fish and images of oceans labeled as water. By being trained on this data, the supervised learning algorithm should be able to later identify unlabeled shark imagesas fish and unlabeled ocean images as water.

A common use case of supervised learning is to use historical data to predict statistically likelyfuture events. It may use historical stock market information to anticipate upcoming fluctuations, or be employed to filter out spam emails. In supervised

learning, tagged photos ofdogs can be used as input data to classify untagged photos of dogs.

## Unsupervised Learning

In unsupervised learning, data is unlabeled, so the learning algorithm is left to find commonalities among its input data. As unlabeled data are more abundant than labeled data, machine learning methods that facilitate unsupervised learning are particularly valuable.

The goal of unsupervised learning may be as straightforward as discovering hidden patterns within a dataset, but it may also have a goal of feature learning, which allows the computationalmachine to automatically discover the representations that are needed to classify raw data.

Unsupervised learning is commonly used for transactional data. You may have a large datasetof customers and their purchases, but as a human you will likely not be able to make sense of what similar attributes can be drawn from customer profiles and their types of purchases. Withthis data fed into an unsupervised learning algorithm, it may be determined that women of a certain age range who buy unscented soaps are likely to be pregnant, and therefore a marketingcampaign related to pregnancy and baby products can be targeted to this audience in order to increase their number of purchases.

Without being told a “correct” answer, unsupervised learning methods can look at complex data that is more expansive and seemingly unrelated in order to organize it in potentially meaningful ways. Unsupervised learning is often used for anomaly detection including for fraudulent credit card purchases, and recommender systems that recommend what products tobuy next. In unsupervised learning, untagged photos of dogs can be used as input data for the algorithm to find likenesses and classify dog photos together.

## PYTHON

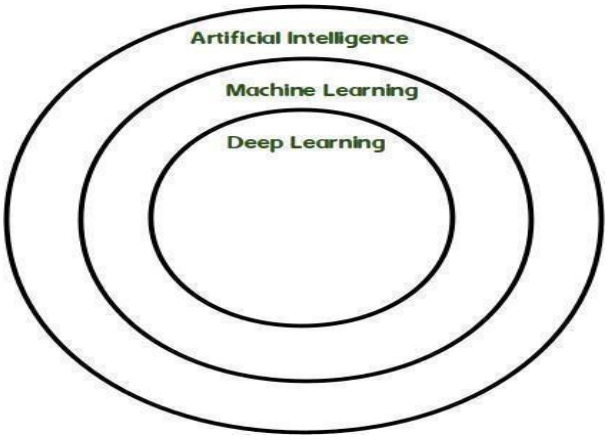
Python is a general-purpose interpreted, interactive, object-oriented, and high-level programming language. An interpreted language, Python has a design philosophy that emphasizes code readability (notably using whitespace indentation to delimit code blocks rather than curly brackets or keywords), and a syntax that allows programmers to express concepts in fewer lines of code than might be used in languages

suchas C++or Java. It provides constructs that enable clear programming on both small

and large scales. Python interpreters are available for many operating systems. CPython, the reference implementation of Python, is open source software and has a community-

based development model, as do nearly all of its variant implementations. CPython is managed by the non- profit Python Software Foundation. Python features a dynamic type system and automatic memory management. It supports multiple programming paradigms,Deep learning is a particular kind of machine learning that achieves great power and flexibilityby learning to represent the world as a nested hierarchy of concepts, with each concept definedin relation to simpler concepts, and more abstract representations computedin terms of less abstract ones.

In human brain approximately 100 billion neurons all together this is a picture of an individualneuron and each neuron is connected through thousand of their neighbours.
The question here is how we recreate these neurons in a computer. So, we create an artificial structure called an artificial neural net where we have nodes or neurons. We have some neuronsfor input value and some for output value and in between, there may be lots of neurons interconnected in the hidden layer.



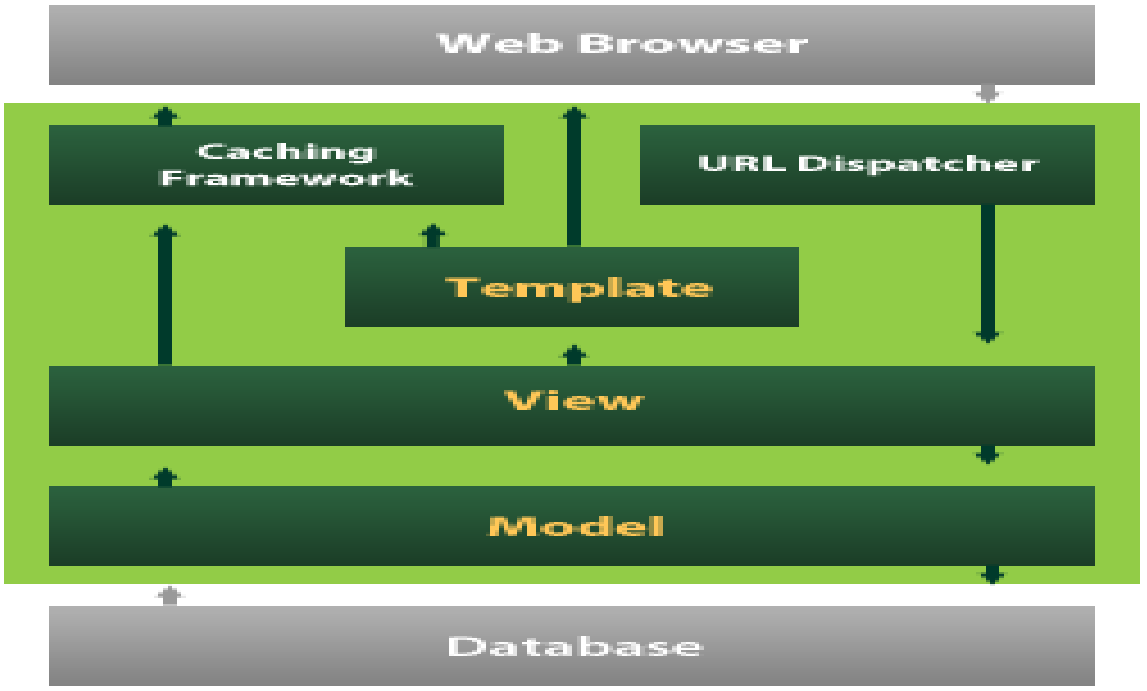

Including object-oriented, imperative, functional and procedural, and has a large and comprehensive standard library

## DJANGO

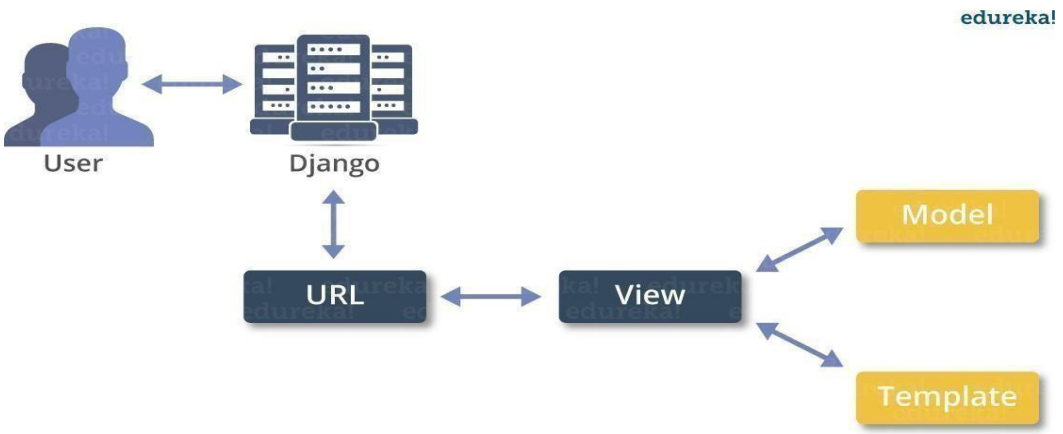
Django is a high-level Python Web framework that encourages rapid development and clean, pragmatic design. Built by experienced developers, it takes care of much of the hassle of Webdevelopment, so you can focus on writing your app without needing to

reinvent the wheel.It’sfree and open source.

Django's primary goal is to ease the creation of complex, database-driven websites. Django emphasizes reusabilityand "pluggability" of components, rapid development, and the principleof don't repeat yourself. Python is used throughout, even for settings files and data models.




Django also provides an optional administrative create, read, update and delete interface that isgenerated dynamically through introspection and configured via admin models.



## 5.3 SOURCE CODE

### 1. FILENAME: ADMIN.PY

```
from django.contrib import admin
```

### 2. FILENAME: APPS.PY

```
from django.apps import AppConfig

class CyberAlertConfig(AppConfig):name = 'cyber_alert'
```

### 3. FILENAME: FORMS.PY

```
from django import forms

from cyber_alert.models import AdminRegister,GiverTransaction

class AdminForm(forms.ModelForm):
email = forms.EmailField(max_length=50)
password = forms.CharField(widget=forms.PasswordInput())

class Meta:
model = AdminRegister
fields = ('adminid', 'name', 'email', 'password', 'phoneno', 'address')

class GiverForm(forms.ModelForm):
```

```
class Meta:

model = GiverTransaction

      fields =
('userid','name','aadharno','address','mobileno','bankname','accountno','branchname','amou
nt','ifsccode','micrcode','date','time','transationid')
```

## 4. FILENAME: 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,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)
```

## 5. NAME:TESTSS.PY

```
from django.test import TestCase

# Create your tests here.
```

## 6. FILENAME:VIEWSS.PY

```
#te from itertools import count

from MySQLdb import Date
from django.contrib import messages
from django.db.models import Count

from django.shortcuts import render, redirect, get_object_or_404

# Create your views here.
from admins.models import Sendquery
```

```
from cyber_alert import forms
from cyber_alert.forms import AdminForm, GiverForm

from cyber_alert.models import GiverTransaction, AdminRegister

def admin_login(request):
    if request.method == "POST":
        name = request.POST.get('name')
        password = request.POST.get('password')
        try:
            check = AdminRegister.objects.get(name=name, password=password)
            request.session['name'] = check.id


            return redirect('giver_transaction')
        except:
            pass



    return render(request, "admin_login.html")


def admin_register(request):
    if request.method == "POST":
        forms = AdminForm(request.POST)
        if forms.is_valid():
            forms.save()
            messages.success(request, 'You have been successfully registered')
            return redirect('admin_login')
```

```
else:
    forms = AdminForm()



return render(request,'admin_register.html',{'form':forms})
def giver_transaction(request):sd=''
   aas=''
   sw=''
   q=''
   name = request.session['name']
   obj = AdminRegister.objects.get(id=name)if request.method == "POST":
   name = request.POST.get('name') aadhar = request.POST.get('aadharno') address =
   request.POST.get('address') mobile = request.POST.get('mobileno') bank =
   request.POST.get('bankname') account= request.POST.get('accountno')
   branch=request.POST.get('branchname')amount=request.POST.get('amount') ifsc=
   request.POST.get('ifsccode') micr=request.POST.get('micrcode')
   date=request.POST.get('date')
   time= request.POST.get('time') transaction=request.POST.get('transactionid')
   sd=date.split("-")

   GiverTransaction.objects.create(userid=obj,day=sd[0],month=sd[1],year=sd[2],name=na
   me,a
   adharno=aadhar,address=address,mobileno=mobile,bankname=bank,accountno=account,
   bran
   chname=branch,amount=amount,ifsccode=ifsc,micrcode=micr,date=date,time=time,tran
   sationid=transaction)
   return render(request,'giver_transaction.html',{'form':sd,'we':q})
   def analyze_page(request):
```

```
name = request.session['name']
admin_obj = AdminRegister.objects.get(id=name)to_name = admin_obj.name
obj = GiverTransaction.objects.filter(name=to_name, )



return render(request, 'analyze_page.html', {'objv': obj})
def viewer(request,chart_type):
chart = GiverTransaction.objects.values('month').annotate(dcount=Count('month'))
return render(request,"viewer.html",{'form':chart,'chart_type':chart_type})
def update(request):
name = request.session['name']
obj = AdminRegister.objects.get(id=name)if request.method == "POST":
Admin_Id = request.POST.get('adminid', '')Name = request.POST.get('name', '')
Email= request.POST.get('email', '') Password = request.POST.get('password', '')
Phone_Number = request.POST.get('phoneno', '')Address = request.POST.get('address',
'')
obj = get_object_or_404(AdminRegister, id=name)obj.adminid = Admin_Id
obj.name = Name obj.email = Email obj.password = Password
obj.phoneno = Phone_Numberobj.address = Address
obj.save(update_fields=["adminid", "name", "email", "password", "phoneno", "address"
])
return redirect('admin_login')
return render(request, 'update.html',{'objc':obj})


def logout_page(request): return redirect(admin_login)

def mydetails(request):
```

```
name = request.session["name"]
obj= AdminRegister.objects.get(id=name)if request.method == "POST":
Admin_Id = request.POST.get('adminid',")Name = request.POST.get('name', ") Email =
request.POST.get('email', ")
```

Password = request.POST.get('password', '') Phone_Number =

request.POST.get('phoneno', '')Address = request.POST.get('address', '')

obj= get_object_or_404(AdminRegister, id=name)obj.adminid = Admin_Id

obj.name = Name obj.email = Email obj.password = Password

obj.phoneno = Phone_Numberobj.address = Address

return render(request, 'mydetails.html', {'objc': obj})

def show(request):

return render(request,'show.html' )def receivealert(request):

name = request.session['name']

admin_obj = AdminRegister.objects.get(id=name)to_name = admin_obj.name

obj=Sendquery.objects.filter(name=to_name)

return render(request, 'receivealert.html',{'de':obj})sts.py

## 7. FILENAME:MANAGE.PY

#!/usr/bin/env pythonimport 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_lineexcept

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 PYTHONPATH environment variable? Did you ""forget to activate a
virtual environment?"
)
    raise execute_from_command_line(sys.argv)
#manage.py
```

# 6. SCREENSHOTS

# 6. SCREENSHOTS

## REGISTRATION PAGE:


Figure 6.1: Registration Page

## LOGIN PAGE:


Figure 6.2:Login Page

## USER SCREENS:

## TRANSACTION PAGE :


Figure 6.3: User Transaction Page

## ANALYZE PAGE:


Figure 6.4 :User Analyze Page

## RECEIVE ALERTS PAGE:

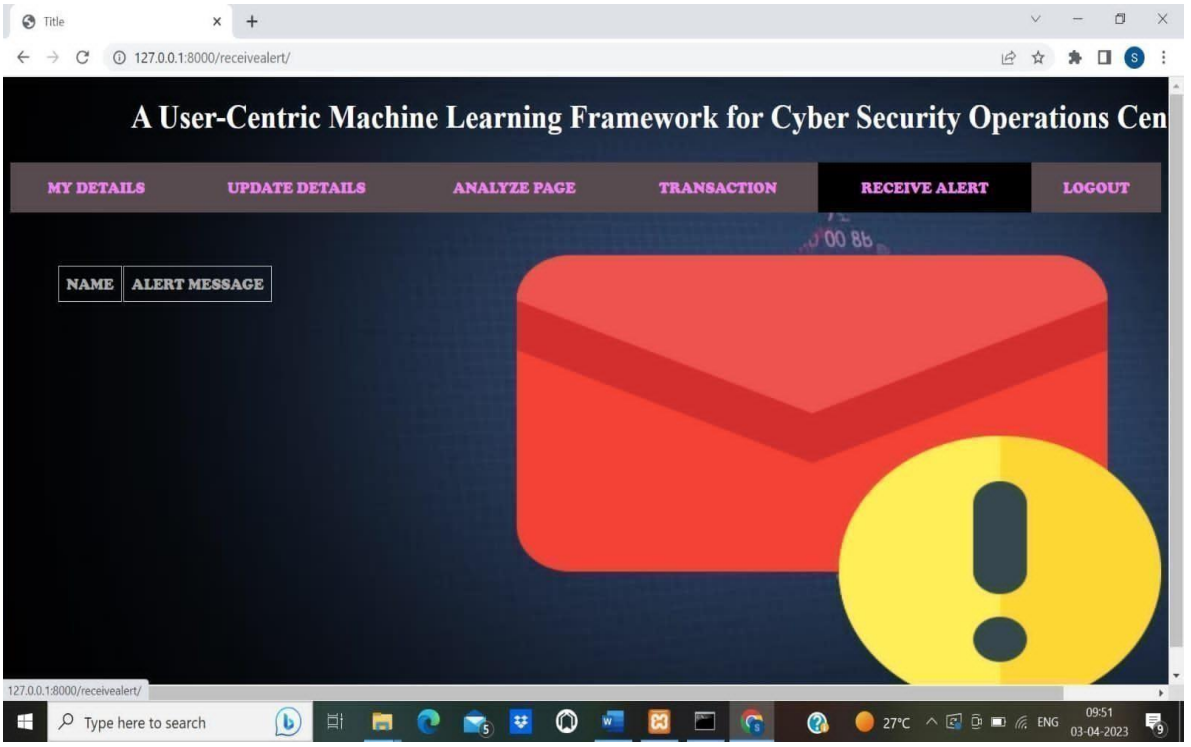



Figure 6.5 :User Receive Alerts Page

## ADMIN SCREENS:
## ANALYZE PAGE:


Figure 6.6: Admin Analyze Page

## RISK USER PAGE:

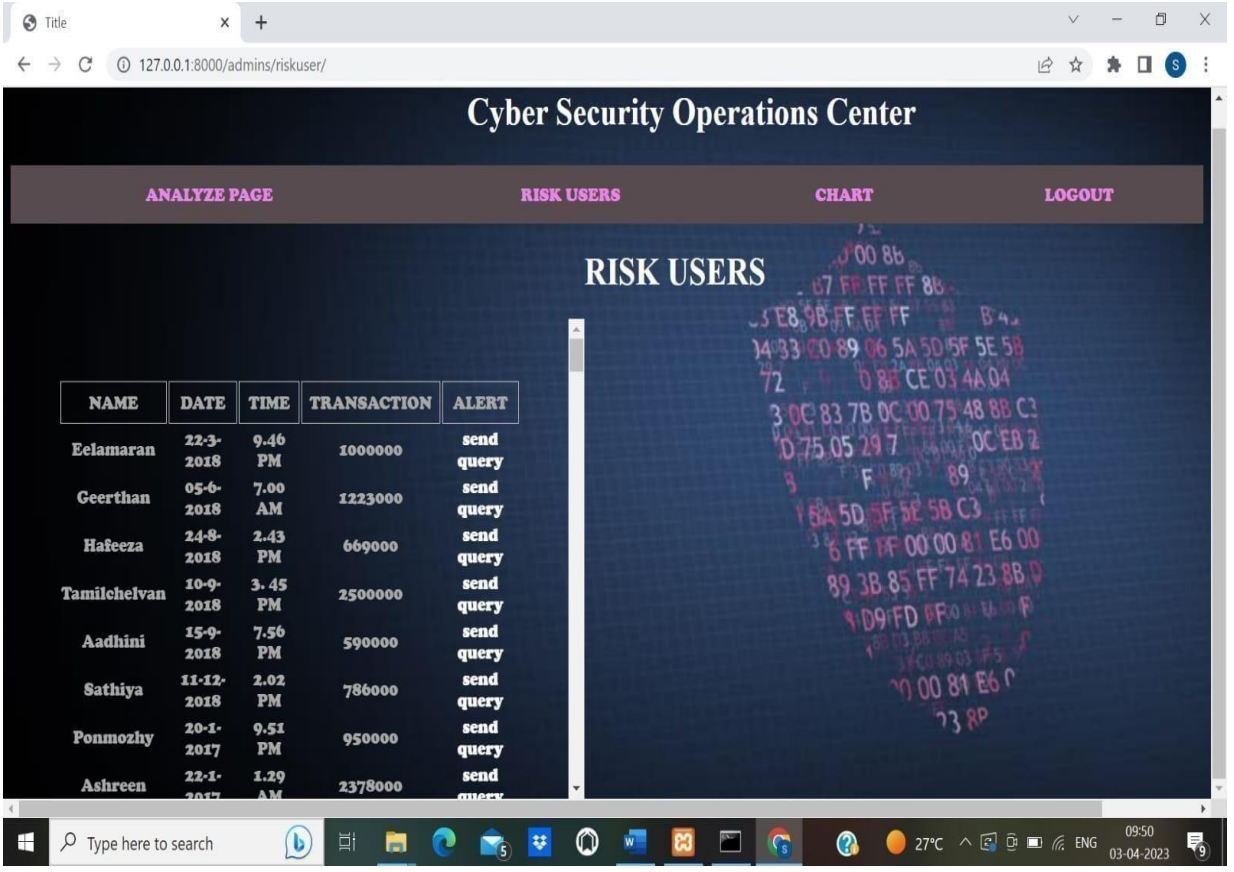



Figure 6.7: Admin Risk Users Page

## SEND QUERY PAGE:

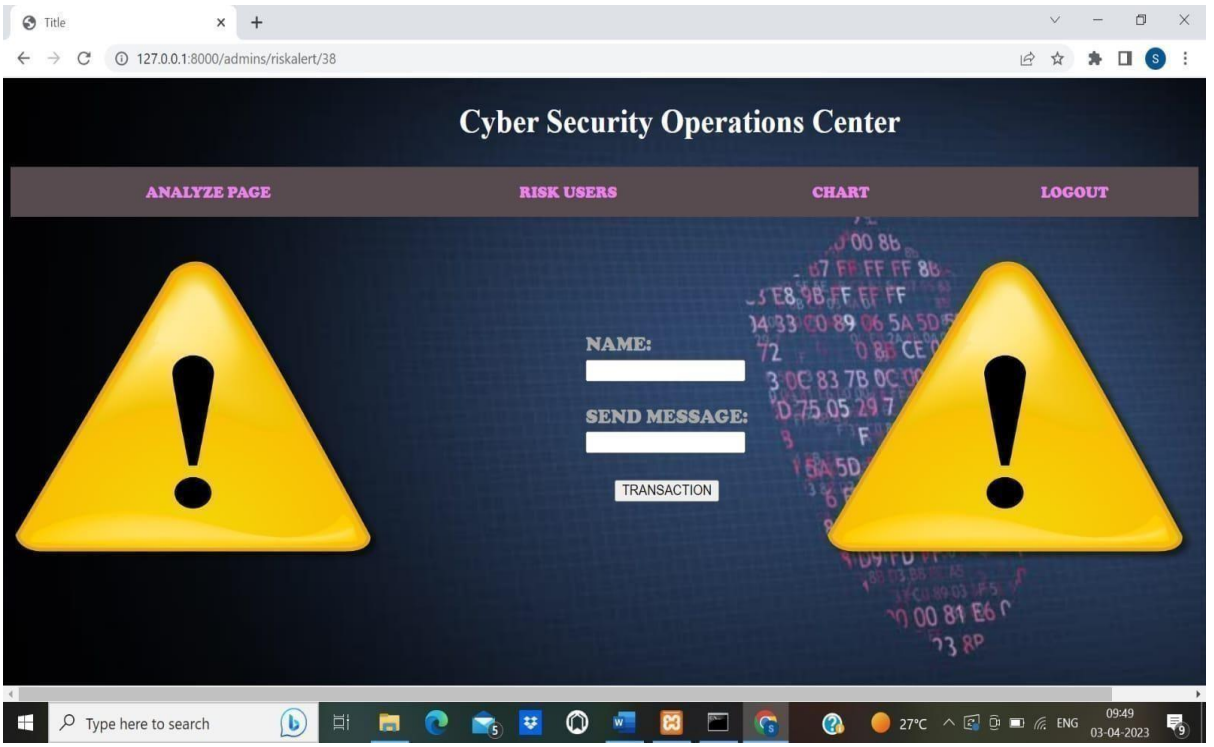



Figure 6.8: Admin Send Query Page

## CHARTS PAGE:

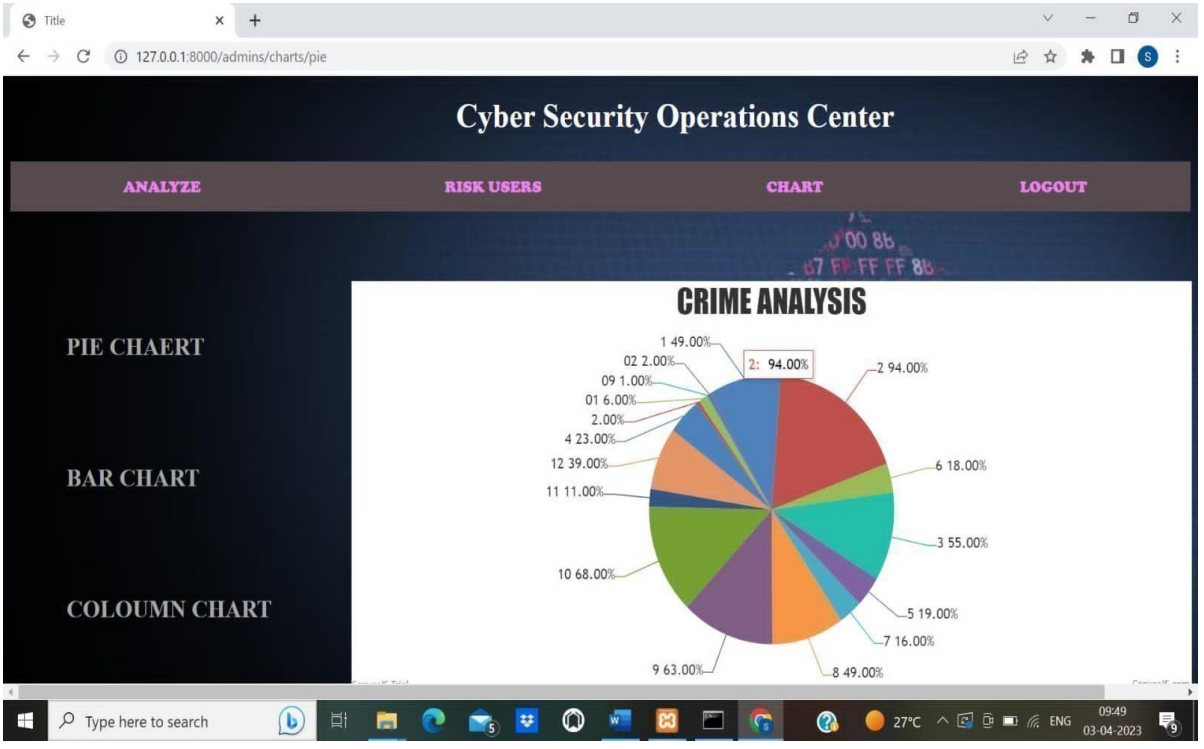



Figure 6.8: Admin Charts Page

# 7.TESTING

# 7. SYSTEM TESTING

## 7.1 INTRODUCTION TO TESTING

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.

### 7.1.1 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 andinternal 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 performbasic tests at component level and test a specific business process, application, and/or systemconfiguration. Unit tests ensure that each unique path of a business process performs accuratelyto the documented specifications and contains clearly defined inputs and expected results.

### 7.1.2 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 wereindividually satisfaction, as shown by successfully unit testing, the combination of

components is correct and consistent. Integration testing is specifically aimed at exposing theproblems that arise from the combination of components.

### 7.1.3 FUNCTIONAL TESTING

Functional tests provide systematic demonstrations that functions tested are available asspecified 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.

### 7.1.4 SYSTEM TESTING

System testing ensures that the entire integrated software system meets requirements. It testsa 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.

### 7.1.5 WHITE BOX TESTING

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

### 7.1.6 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 softwareunder 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.

## UNIT TESTING

Unit testing is usually conducted as part of a combined code and unit test phase of the softwarelifecycle, although it is not uncommon for coding and unit testing to be conducted astwo distinct phases.

**Test strategy and approach**

Field testing will be performed manually and functional tests will be written in detail.

**Test objectives**

* All field entries must work properly.
* Pages must be activated from the identified link.
* The entry screen, messages and responses must not be delayed.

**Features to be tested**

* Verify that the entries are of the correct format
* No duplicate entries should be allowed
* All links should take the user to the correct page.

## INTEGRATION TESTING

Software integration testing is the incremental integration testing of two or more integratedsoftware components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g.components in a software system or – one step up – software applications at the company level
– interact without error.

**Test Results:** All the test cases mentioned above passed successfully. No defects encountered.

### 7.1.7 ACCEPTANCE TESTING

User Acceptance Testing is a critical phase of any project and requires significant participationby the end user. It also ensures that the system meets the functional requirements.

**Test Results:** All the test cases mentioned above passed successfully. No defectsencountered.

Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

# Certificate of Publication

This is to certify that the paper entitled

## A NOVEL CYBER SECURITY FRAMEWORK FOR ONLINE FRUAD TRANSACTIONS DETECTION USING MACHINE LEARNING

**Authored By**

**Dr .K. Srujan Raju**

From

Professor, Dept. of CSE, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

**Has Been Published in**

**JICR JOURNAL, Volume XV, Issue III, March/2023**

Dr. R. Rezwana Begum, Ph.D Editor-In-Chief
JICR JOURNAL

6.2 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

# 8. CONCLUSION AND FUTURE SCOPE

# 8. CONCLUSTION AND FUTURE SCOPE

## 8.1 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. . Evenwith 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 theneurological modelof modeling is 5 times that of the current rule-based system. To improve the detection precisionsituation, we will examine other learning methods to improve the data acquisition, daily modelrenewal, 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.

## 8.2 FUTURE SCOPE

The future scope for this type of system is significant. As the amount of data generated by enterprise systems continues to grow, it becomes increasingly challenging to detect and prevent dangerous user behaviour using traditional rule-based systems. Machine learning offers a promising solution to this problem by enabling automated detection of anomalous behaviour based on patterns and trends in the data.In the future, this type of system could be further developed to incorporate more advanced machine learning algorithms and techniques, such as deep learning and neural networks. This could lead to even greater accuracy and efficiency in detecting and preventing dangerous user behaviour. Additionally, the system could be integrated with other security measures, such as threat intelligence feeds and incident response protocols, to provide a more comprehensive security solution. Furthermore, the system could be adapted to other industries beyond enterprise security, such as healthcare, finance, and government, where similar challenges exist in detecting and preventing malicious behaviour. Overall, the future scope for this type of this type of machine learning system is quite promising, with potential for continued innovation and development.

# 9. REFERENCES

# 9. REFERENCES

[1] Cheshta Rani, Shivani Goel. An Expert System for Cyber Security Attack Awareness, International Conference on Computing, Communication, and Automation (ICCCA2015) ISBN:978-1- 4799-8890-7/15/$31.00 ©2015 IEEE 242 CSAAES.

[2] S. Poonia, A. Bhardwaj, G. S. Dangayach, (2011) "Cyber Crime: Practices and Policies forIts Prevention", The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management, Vol. 19, No. SP1. Journal of Xi'an University of Architecture & Technology Volume XII, Issue V, 2020 ISSN No : 1006-7930 Page N

[3] Dr. Sunil Bhutada, PreetiBhutada.Applications of Artificial Intelligence in Cybersecurity International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018 All Rights Reserved © 2018 IJERCSE 214.

[4] NIKITA RANA, SHIVANI DHAR, PRIYANKA JAGDALE, NIKHIL JAVALKAR. Implementation of An Expert System for the Enhancement of ECommerce Security International Journal of Advances in Science Engineering and Technology, ISSN: 2321-9009Volume- 2, Issue-3, July-2014

[5] M.M. Gamal, B. Hasan, and A.F. Hegazy, "A Security Analysis Framework Powered by an Expert System," International Journal of Computer Science and Security (IJCSS), Vol. 4, no. 6, pp. 505-527, Feb. 2011.

[6] K. Goztepe, "Designing a Fuzzy Rule-Based Expert System for Cyber Security," International Journal Of Information Security Science, vol.1, no.1, 2012.

[7] D. Welch, "Wireless Security Threat Taxonomy," Information Assurance Workshop. IEEE Systems, Man and Cybernetics Society, pp 76-83, June 2003.

[8] VidushiSharma, SachinRai, AnuragDev" A Comprehensive Study of Artificial Neural Networks" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 10, October 2012.

[9] ShaiquaJabeen, Shobhana D. Patil, Shubhangi V. Bhosale, Bharati M. Chaudhari, Prafulla

S. Patil" A Study on Basics of Neural Network" International Journal of Innovative Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2017.

[10] Nalini, M. and Anbu, S., "Anomaly Detection Via Eliminating Data Redundancy and Rectifying Data Error in Uncertain Data Streams", Published in International Journal of Applied Engineering Research (IJAER), Vol. 9, no. 24, 2014.

[11] Nalini, M. and Anvesh Chakram, "Digital Risk Management for Data Attacks against State Evaluation", Published in International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 8, Issue no. 9S4, pp. 197-201,July 2019.[DOI:10.35940/ijitee.I1130.0789S41 9]

[12] Nalini, M., and Uma Priyadarshini, To Improve the Performance of Wireless Networks for Resizing the Buffer, Proceedings of the 2019 international IEEE Conference on Innovationsin Information and Communication Technology, Apr 2019.[DOI >10.1109/ICIICT1.2019.8741406]

[13] Shiny Irene D., G. Vamsi Krishna and Nalini, M., "Era of quantum computing- An intelligent and evaluation based on quantum computers", Published in International Journal ofRecent Technology and Engineering (IJRTE), Vol. 8, Issue no.3S, pp. 615- 619, October

## 9.1 GITHUB LINK

# A NOVEL CYBER SECURITY FRAMEWORK FOR ONLINE FRUAD TRANSACTIONS DETECTION USING MACHINE LEARNING

[1]B. Hemanth Naidu, [2]G. Pallavi, [3]P. Vishala Reddy, [4]Dr .K. Srujan Raju
[1,2,3]B. Tech Student, Dept. of CSE, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.
197r1a0505@cmrtc.ac.in , 197r1a0512@cmrtc.ac.in , 197r1a0543@cmrtc.ac.in
[4] Professor, Dept. of CSE, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.
ksrujanraju@gmail.com

**ABSTRACT: With the rapid development of Internet technology, the scale of online transactions is constantly expanding. At the same time, the related network transaction fraud problem has become more significant. Compared with the credit card transaction, the network transaction has the characteristics of low cost, wide coverage and high frequency, which makes the detection of fraud more complex. Financial fraud cases are on the rise even with the current technological advancements. Due to the lack of inter-organization synergy and because of privacy concerns, authentic financial transaction data is rarely available. Cyber security has a lot of advancements and procedures which are intended to secure PCs, networks, projects, and information from assaults and unapproved access, change, or obliteration. On the other hand ML techniques have shown significant results in prediction, detection and classification tasks. Hence in this work, a novel cyber security framework for online fraud transactions detection using Machine Learning is presented. The Support Vector Machine (SVM) is used to detect the risks and Frauds in online Transactions. This approach will achieve better results in terms of detection accuracy.**

**KEYWORDS: Cyber Security Credit Card, Online Transaction, Machine Learning.**

## I. INTRODUCTION

With the advancement of cutting-edge technology and global connectivity, fraud has risen dramatically. There are two ways to identify fraud: prevention and detection. By serving as a layer of defense, prevention helps to keep fraudsters at bay [1]. With the increasingly in-depth integration of the Internet and social life, the Internet is changing how people learn and work, but it also exposes us to increasingly serious security threats.

How to identify various network attacks, particularly not previously seen attacks, is a key issue to be solved urgently. Cyber security incidents will cause significant financial and reputation impacts on enterprise [3]. 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. 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.

Cyber security is a set of technologies and processes designed to protect computers, networks, programs and data from attacks and unauthorized access, alteration, or destruction. A network security system consists of a network security system and a computer security system. Each of these

systems includes firewalls, antivirus software, and intrusion detection systems (IDS). IDSs help discover, determine and identify unauthorized system behavior such as use, copying, modification and destruction.

The popularization of credit cards is across many fields such as healthcare, shopping, etc. Because of credit cards, the online transaction has become more convenient and more accessible. However, fraud transaction impacts the massive loss of capital every year which might increase in the coming year. The system for detecting the fraud might be composed of a manual process and the expertise algorithm for detecting the fraud automatically. (e automatic operation can be based upon all previous ways of fraud transactions happened [4].

The manual method is estimated by different fraud investigators who check the separate transaction and generate binary feedback on every transaction. Fraud cases in the transaction are the primary barrier while enhancing the e-commerce and also cause a massive loss in the economy. Hence, detection of fraud is essential while doing transactions in an online environment [2].

Detection of fraud is the process of analyzing the behavior of card holders' transactions to know whether the conducted transaction is genuine. Frauds in credit cards signify the illegal use of information in credit cards and completing a transaction. While transacting physically, the involvement of credit card is there while the digital transaction is conducted utilizing the Internet or a telephone as information such as card number, its verification number, and its expiry date is collected through different mean.

Traditional fraud detection mostly adopts statistical and multi-dimensional analysis techniques. Since they are verification techniques, it is difficult to obtain the laws hidden behind the transaction data. The big data technology and machine learning algorithm provide efficient detection methods for transaction fraud detection. Compared to the traditional statistical methods, machine learning can represent important features through a large amount of data, which cannot be described by the former [5].

Hence, in this work, a novel cyber security framework for online fraud transactions detection using Machine Learning is presented. The remaining work is organized as follows: The section II describes the literature survey. The section III presents a novel cyber security framework for online fraud transactions detection using Machine leaning. The section IV evaluates the result analysis. Finally the section V ends with conclusion.

## II. LITERATURE SURVEY

FeiWang, Nan Yang, P. Mohamed Shakeel, Vijayalakshmi Saravanan et. al., [5] describes Machine learning for mobile network payment security evaluation system. Machine Learning-Assisted Secure Mobile Electronic Payment Framework (ML-SMEPF) is proposed to detect the presence of malware, authentication issues, and fraud detection in mobile transactions. Here, the Efficient Random Oracle Model is introduced to detect the presence of malware on a host system and multi-factor authentication challenges posed during mobile payments. Mutual Mobile Authentication model is incorporated with ML-SMEPF, to identify the type of fraud detection which ensures a safe and secure mobile payment platform. The simulation analysis is performed based on accuracy ratio, security factor, performance, and cost factor proves the reliability of the presented framework.

Dalila Boughaci, Abdullah A.K. Alkhawaldeh et. al., [7] describes Enhancing the security of financial

transactions in Blockchain by using machine learning techniques:towards a sophisticated security tool for banking and finance. The main idea is applied to the Bitcoin system where the public Elliptic dataset from Kaggle is used as a benchmark. Since the latter is not all labeled, the k-means algorithm is used to partition the unlabeled data into two main clusters while the labeled data are moved to their corresponding clusters. Then, four machine learning techniques are used to classify all the data. This system shows promising results in particular when combining k-means with the random forest classifier.

Abdulrahman Al-Abassi, Hadis Karimipour, Ali Dehghantanha, Reza M. Parizi et. al., [8] presents An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. deep learning model to construct new balanced representations of the imbalanced datasets. The new representations are fed into an ensemble deep learning attack detection model specifically designed for an ICS environment. The proposed attack detection model leverages Deep Neural Network (DNN) and Decision Tree (DT) classifiers to detect cyber-attacks from the new representations. The performance of the proposed model is evaluated based on 10-fold cross-validation on two real ICS datasets. The results show that the proposed method outperforms conventional classifiers, including Random Forest (RF), DNN, and AdaBoost, as well as recent existing models in the literature. The proposed approach is a generalized technique, which can be implemented in existing ICS (Industrial Control Systems) infrastructures with minimum effort.

Charles Feng, Shuning Wu, Ningwei Liu et. al., [9] describes A User-Centric Machine Learning Framework for Cyber Security Operations Center. A user centric machine learning framework is developed for the cyber security operation center in real enterprise environment. This approach discussed the typical data sources in SOC, their work flow, and how to leverage and process these data sets to build an effective machine learning system. Symantec SOC production environment is built 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. The average lift on top 20% predictions for multi neural network model is over 5 times better than earlier rule-based system.

John O. Awoyemi, Adebayo O. Adetunmbi, Samuel A. Oluwadare et. al., [10] describes Credit card fraud detection using machine learning techniques: A comparative analysis. This paper investigates the performance of naïve bayes, k-nearest neighbor and logistic regression on highly skewed credit card fraud data. Dataset of credit card transactions is sourced from European cardholders containing 284,807 transactions. A hybrid technique of under-sampling and oversampling is carried out on the skewed data. The three techniques are applied on the raw and preprocessed data. The work is implemented in Python. The performance of the techniques is evaluated based on accuracy, sensitivity, specificity, precision, Matthews correlation coefficient and balanced classification rate. The comparative results show that k-nearest neighbour performs better than naïve bayes and logistic regression techniques.

## III. NOVEL CYBER SECURITY FRAMEWORK FOR ONLINE FRAUD TRANSACTIONS DETECTION

In this section a novel cyber security framework for online fraud transactions detection using Machine Learning is presented.

The novel cyber security framework 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. Online money transactions have always been the target of criminals and are affected by security threats because of their complexity and cyber-security connectivity.

The presented mainly contains two modules namely user module and admin module which are shown in Fig. 1 and 2. The user is login with their account through their registered mobile number, bank account and credit card details. The users login to their accounts and check their account details for further processing. The user is capable to do money transactions to other persons, paying the bills, shopping, booking tickets. Etc. Through the admin module, the online transactions are analyzed, risks and frauds are detected and alert message will be provided.

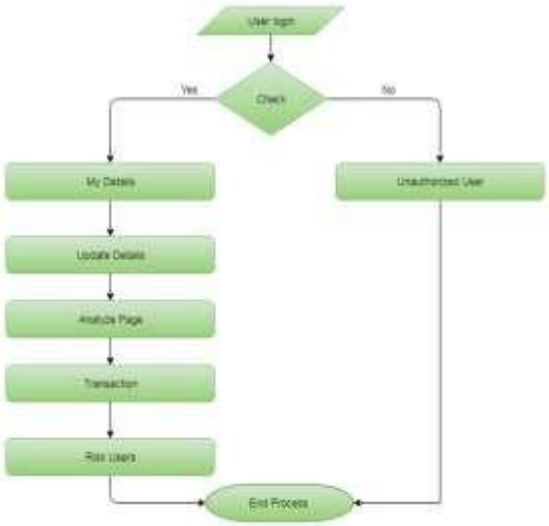



**Fig. 1: User Module**

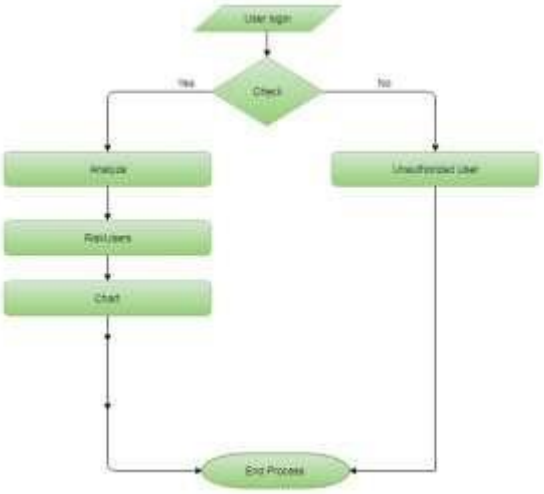



**Fig. 2: Admin Module**

Firstly, the source of the dataset is collected from UCI Machine Learning Repository. The dataset holds the information related transaction conducted through credit cards as a default payment gateway of the different customers in Taiwan. (e dataset has the detail of transaction which has occurred in the year 2015 and consists of 30000 different customer data and nearly 3 lakhs of transaction data. The characteristic of the dataset is multivariate, and its entire attributes are accurate and integer.

Data pre-processing, a component of data preparation, describes any type of processing performed on raw data to

prepare it for another data processing procedure. Data pre-processing can refer to manipulation or dropping of data before it is used in order to ensure or enhance performance, and is an important step. After pre-processing features are extracted.

Some features may not help the detection process and may increase the detection process complexity. So, the removal of features that have a small variance might even lead to better results since these dimensions consist mostly of noise and would, therefore, reduce the weight of features that contain more information. The principal component analysis (PCA) is used to remove these features. Therefore, for each instance, only a subset of the components of the feature vector will be used as input to the detection algorithm i.e. SVM (Support Vector Machine).

Support Vector Machine or SVM is one of the most popular Supervised Learning algorithms, which is used for Classification as well as Regression problems. However, primarily, it is used for Classification problems in Machine Learning. The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyperplane. SVM chooses the extreme points/vectors that help in creating the hyperplane. These extreme cases are called as support vectors, and hence algorithm is termed as Support Vector Machine. Here, in this analysis, SVM is used to detect the frauds and risks in online transactions.

## IV. RESULT ANALYSIS

In this section a novel cyber security framework for online fraud transactions detection using Machine Learning is implemented. The result analysis of presented approach is discussed in this section. The Fig. 3 shows the user transaction page.


**Fig. 3: User Transaction Page**

The Fig. 4 shows the user analyze page.


**Fig. 4: User Analyze page**

The fig. 5 shows the alert message.

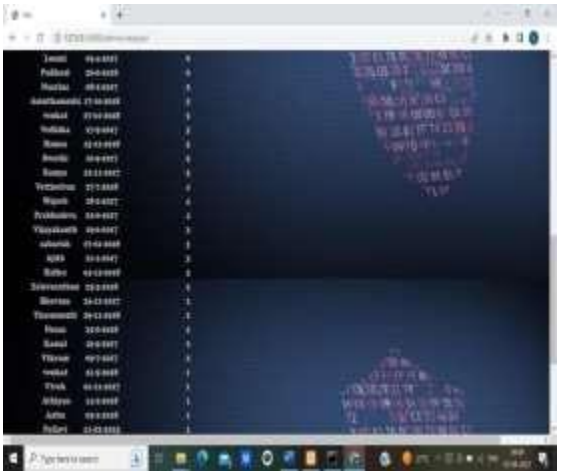
**Fig. 5: Alert message**

The Fig. 6 shows the admin analyze page.


**Fig. 6: Admin's Analyze page**

The Fig. 7 shows the risk users page of admin.


**(a)**



**(b)**

**Fig. 7(a) & (b): Admin's risk user page**

The Fig. 8 shows the Admins query page.


**Fig. 8: Admin's query page**

The Fig. 9 shows admin's chart page.


**Fig. 9: Admin's chart page**

Hence this approach has effectively detects the risks and frauds.

## V. CONCLUSION

Mobile payment systems in various contexts are ever more important in modern information technology as an alternative payment process. The benefits of these metrics are flexibility, perceived utility, durability, comfort, and mobility. In this work, a novel cyber security framework for online fraud transactions detection using Machine Learning is presented. With the diversification of online transactions, machine learning is applied to more and more anti-fraud processing. The dataset related to a credit card is available publicly is used. The data is preprocessed to improve the accuracy. The features are extracted from pre-processed data and extracted features are applied to Support Vector Machine Classifier. The SVM detects the risks and

frauds of a online transaction. This approach has detected the risks very effectively. Therefore this approach is very useful for real time frauds and risks in online transactions.

## VI. ACKNOWLEDGEMENT

We thank CMR Technical Campus for supporting this paper titled "A Novel Cyber Security Framework for Online Fruad Transactions Detection Using Machine Learning", which provided good facilities and support to accomplish our work. Sincerely thank our Chairman, Director, Deans, Head Of the Department, Department Of Computer Science and Engineering, Guide and Teaching and Non- Teaching faculty members for giving valuable suggestions and guidance in every aspect of our work

## VII. REFERENCES

[1]Shayan Wangde, Raj Kheratkar, Zoheb Waghu, Prof. Suhas Lawand, "Online Transaction Fraud Detection System Using Machine Learning & E-Commerce", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 09 Issue: 04, Apr 2022

[2] Tahmid Hasan Pranto, Kazi Tamzid Akhter Md. Hasib, Tahsinur Rahman, Akm Bahalul Haque, A. K. M. Najmul Islam, Rashedur M. RAHMAN, "Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach", IEEE Access ( Volume: 10), DOI: 10.1109/ACCESS.2022.3198956

[3] M. Sathana, M.Hemamalini, "A Thread based Machine Learning Framework for Cyber Security Operations Center", International Journal of Research Publication and Reviews, Vol 3, no 5, pp 3683-3687, May 2022

[4] Abolfazl Mehbodniya, Izhar Alam ,Sagar Pande, Rahul Newarer, Kantilal Pitambar Rane, Mohammad Shabaz, and Mangena Venu Madhavan, "Financial Fraud Detection in Healthcare Using Machine Learning and Deep Learning Techniques", Hindawi Security and Communication Networks, Volume 2021, Article ID 9293877, 8 pages, doi:10.1155/2021/9293877

[5] Bocheng Liu, Xiang Chen and Kaizhi Yu, "System Based on Machine Learning", Journal of Physics: Conference Series, 2021, 012054, doi:10.1088/1742-6596/2023/1/012054

[6] FeiWang, Nan Yang, P. Mohamed Shakeel, Vijayalakshmi Saravanan, "Machine learning for mobile network payment security evaluation system", Trans Emerging Tel Tech. 2021;e4226., 2021, doi:10.1002/ett.4226

[7] Dalila Boughaci, Abdullah A.K. Alkhawaldeh, "Enhancing the security of financial transactions in Blockchain by using machine learning techniques:towards a sophisticated security tool for banking and finance", 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)

[8] Abdulrahman Al-Abassi, Hadis Karimipour, Ali Dehghantanha, Reza M. Parizi, "An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System", IEEE Access ( Volume: 8), 2020, DOI: 10.1109/ACCESS.2020.2992249

[9] Charles Feng, Shuning Wu, Ningwei Liu, "A User-Centric Machine Learning Framework for Cyber Security Operations Center", 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), DOI: 10.1109/ISI.2017.8004902

[10] John O. Awoyemi, Adebayo O. Adetunmbi, Samuel A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis", 2017 International Conference on Computing Networking and Informatics (ICCNI), DOI: 10.1109/ICCNI.2017.8123782

Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

# Certificate of Publication

This is to certify that the paper entitled

## A NOVEL CYBER SECURITY FRAMEWORK FOR ONLINE FRUAD TRANSACTIONS DETECTION USING MACHINE LEARNING

**Authored By**

**Dr .K. Srujan Raju**

From

Professor, Dept. of CSE, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

Has Been Published in

**JICR JOURNAL, Volume XV, Issue III, March/2023**

Dr. R. Rezwana Begum, Ph.D Editor-In-Chief
JICR JOURNAL

Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

# Certificate of Publication

This is to certify that the paper entitled

## A NOVEL CYBER SECURITY FRAMEWORK FOR ONLINE FRUAD TRANSACTIONS DETECTION USING MACHINE LEARNING

Authored By

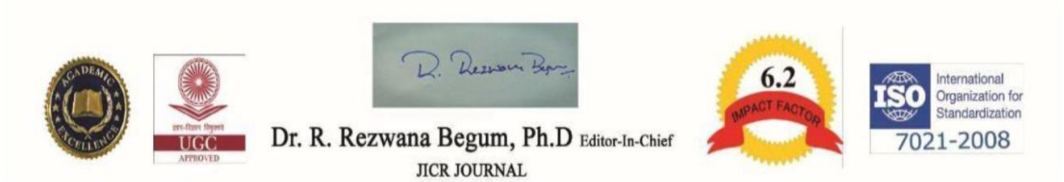
**B. Hemanth Naidu**

From

B. Tech Student, Dept. of CSE, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

Has Been Published in

**JICR JOURNAL, Volume XV, Issue III, March/2023**



Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

# Certificate of Publication

This is to certify that the paper entitled

## A NOVEL CYBER SECURITY FRAMEWORK FOR ONLINE FRUAD TRANSACTIONS DETECTION USING MACHINE LEARNING

Authored By

**P. Vishala Reddy**

From

B. Tech Student, Dept. of CSE, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

Has Been Published in

**JICR JOURNAL, Volume XV, Issue III, March/2023**

Dr. R. Rezwana Begum, Ph.D Editor-In-Chief
JICR JOURNAL

6.2 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

# Certificate of Publication

This is to certify that the paper entitled

## A NOVEL CYBER SECURITY FRAMEWORK FOR ONLINE FRUAD TRANSACTIONS DETECTION USING MACHINE LEARNING

Authored By

**G. Pallavi**

From

B. Tech Student, Dept. of CSE, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

Has Been Published in

**JICR JOURNAL, Volume XV, Issue III, March/2023**

Dr. R. Rezwana Begum, Ph.D Editor-In-Chief
JICR JOURNAL

6.2 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008