

ONLINE FRAUD DETECTION

18CSC206J /SOFTWARE ENGINEERING AND PROJECT MANAGEMENT REPORT

Submitted by

N.SAI SADWIK REDDY [RA2111030020053]

SHIVNATH CHIRANJEEVI [RA2111030020045]

K.VENKATA RAMA SUJAL [RA2111030020030]

Under the guidance of

Dr.M.S.MINU

(Assistant Professor, Department of Computer Science and Engineering)

in partial fulfillment for the award of the degree

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

of

FACULTY OF ENGINEERING AND TECHNOLOGY



SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

RAMAPURAM CAMPUS, CHENNAI -600089

MAY 2023

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University U/S 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this is the bonafide report of work done by **N.SAI SADWIK REDDY [RA2111030020053]**, **SHIVNATH CHIRANJEEVI [RA2111030020045]**, **K.VENKATA RAMA SUIJAL [RA2111030020030]** of IV Semester B.Tech Computer Science and Engineering during the academic year 2022-2023 Even Semester in ***18CSC206J/SOFTWARE ENGINEERING AND PROJECT MANAGEMENT***

SIGNATURE

Dr.M.S.MINU

Designation,

Computer Science and Engineering,
SRM Institute of Science and Technology,
Ramapuram Campus, Chennai.

SIGNATURE

Dr. K.RAJA,M.E., Ph.D.,

Professor and Head

Computer Science and Engineering,
SRM Institute of Science and Technology,
Ramapuram Campus, Chennai.

Submitted for the End Semester Practical Examination held on -----
at SRM Institute of Science and Technology, Ramapuram Campus, Chennai -600089.

Examiner- 1

Examiner- 2

Table of Contents

Exp.No	Date	Content	Page No	Signature
1	18-01-2023	Problem Statements Identify the Software Project Create Business Case Arrive at a Problem Statement		
2	25-01-2023	Stakeholders & Process Models Stakeholder and User Description Identifying Stakeholders User story Identify the Appropriate Process Model Arrive at a Problem Statement Comparative Study with Agile		
3	01-02-2023	Identifying The Requirements From Problem Statement Requirements Elicitation Feasibility Study Functional Requirements Non-Functional Requirements System Requirements		
4	08-02-2023	Project Plan and Project Effort Based On Resources Project Plan Identify Job Roles and Responsibilities		
5	15-02-2023	Project Effort Based On Resources Work Breakdown Structure Risk Analysis		
6	22-02-2023	Estimation of Project Metric's Function Point Analysis COCOMO Model		

7	01-03-2023	Design System Architecture		
8	08-03-2023	Modeling UML Use Case Diagrams & Capturing Use Case Scenarios Use case diagrams Identifying Actors Use Case Association between Actors and Use Cases Use Case Relationships Include Relationship Extend Relationship Generalization Relationship		
9	15-03-2023	E-R modeling from the Problem Statements Entity Relationship Model Entity Set and Relationship Set Attributes of Entity Keys Weak Entity		
10	22-03-2023	Identifying Domain Classes from the Problem Statements Domain Class Using Generalization Using Subclasses		
11	29-03-2023	Statechart & Activity Modeling Statechart Diagrams State Transition Action Activity Diagrams Components of an Activity Diagram		

12	30-03-2023	Modeling UML Class Diagram & Sequence Diagrams Class diagram Class Relationships Sequence diagram Object Life-line bar		
13	05-04-2023	Modelling Data Flow Diagrams Data Flow Diagram Context diagram and levelling DFD		
14	12-04-2023	Implementation Addition of New Requirement Addition of New Issue		
15	13-04-2023	Estimation of Test Coverage Metrics & Structural Complexity Control Flow Graph McCabe's Cyclomatic Complexity Optimum Value of Cyclomatic Complexity		
16	13-04-2023	Designing Test Suites Software Testing Testing Frameworks Master Test Plan Manual Testing		
17	13-04-2023	Deployment Report		
18	13-04-2023	Conclusion		
19	13-04-2023	References		

EXPERIMENT – 1

DATE :	18/1/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATARAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

BUSINESS CASE :

THE PROJECT :

In this project ,we describe the online frauds and create a awareness among the people and also Explain how to be cautious from these frauds.

- Internet fraud involves using online services and software with access to the internet to defraud or take advantage of victims.
- The term "internet fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing.
- Internet scams that target victims through online services account for millions of dollars worth of fraudulent activity every year.

HISTORY :

Internet fraud began appearing in 1994 with the start of E-COMMERCE. The first trend to be seen was the use of “Famous Names” to commit the fraud. In May 2000, the economic offences wing, IPR section crime branch of Delhi police registered its first case involving theft of Internet hours.

TYPES OF INTERNET/ONLINE FRAUD :

Cyber criminals use a variety of attack vectors and strategies to commit internet fraud. This includes malicious software, email and instant messaging services. These are broken into several types: 1) PHISHING

2) DATA BREACH

3) DENIAL OF SERVICE

4) MALWARE

5) RANSOMWARE.

WAYS TO SAFEGUARD OURSELVES FROM FRAUD :

1) Use Smart, Verified Apps Only....

2) Browse Secure and Authorized Websites Only....

3) Use Secure Internet Connections....

4) Be Vigilant When Using the Card....

5) Update Your Computer and Mobile Security...



Problem Statement :

Section 01: Problem description

Online fraud is the use of the internet to defraud or take financial advantage of you. Fraudsters do this by accessing your online bank account or by presenting you with false offers in order to get you to transfer money or provide them with your card details.

The internet is part of our daily lives for shopping, banking and connecting socially. While it brings many opportunities it also allows criminals attempt crimes from a distance reducing their chances of being caught.

Online fraud comes in many forms. It ranges from viruses that attack computers with the goal of retrieving personal information, to email schemes that lure victims into wiring money to fraudulent sources, to “phishing” emails that purport to be from official entities (such as banks or the Internal Revenue Service) that solicit personal information from victims to be used to commit

identity theft, to fraud on online auction sites (such as Ebay) where perpetrators sell fictional goods. The methods used by perpetrators of online fraud are constantly evolving.

Section 02 : Problem Constraints

PURPOSE AND NEED:

The purpose of fraud may be monetary gain or other benefits, for example by obtaining a passport, Financial gain or steal data from the company to benefit their personal gain and needs.

Issues of fraud:

People affected by fraud against public bodies suffer from social problems such as loss of reputation, feelings of vulnerability, isolation and exposure. Fraud can impact on a victim's mental health, resulting in anxiety, depression and suicide.

Cause of online fraud:

There are two main reasons that online fraud occurs as often as it does: It is fairly easy for hackers to steal the needed data. For fraudsters, it is easy to buy this information on the black market. Lack of prosecution for this type of crime.

Most common online fraud:

Copycat government websites. Some scams involve websites designed to look like official government websites such as HMRC

Dating and romance scams

Holiday frauds

Mandate fraud

Payment fraud

Friendly fraud

Section 03: Resources (Tools)

Fraudster hunger for your Social Security number, date and place of birth, mother's maiden name, and other identifiers. They siphon information from data breaches, the dark web and public sources such as social media sites and employee directories here are some tools used by fraudsters to commit fraud :

- 1)SPOOFING
- 2)FAKE PROFILES
- 3)FAKE PHOTOS
- 4)FAKE IDENTITY
- 5)FAKE CLAIMS
- 6)COMPUTER POP-UP
- 7)ROBOCALLS
- 8)LEAD LISTS
- 9)SECRECY
- 10) PERSUASION

EXPERIMENT – 2

DATE :	25/1/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

STAKE HOLDERS :

Internet fraud is a rapidly growing threat to the entire world and with more and more devices being connected to internet, stakeholders need to come up with plans to counter this threat. The various stakeholders in internet fraud are law enforcement agencies, internet security agencies, academia, internet service providers, domain registrars, policy makers, researchers and (last but not the least) the victims. Some of the measures these stakeholders can take to protect themselves and turn the tide against fraudsters are :

- Recognition of threat: what constitutes internet fraud needs to be recognized by all the stakeholders.
- Concerted efforts of all the stakeholders are required to protect us against future frauds. Efforts of one or a few stakeholders will not help the situation.
- Strong, enforceable laws are needed to safeguard against frauds. The laws should be strict enough to be a deterrence against future offenses.
- Technical measures need to be continually devised and updated to prevent fraud from happening in the Internet fraud is a rapidly growing threat to the entire world and with more and more devices being connected to internet, stakeholders need to come up with plans to counter this threat. The various stakeholders in internet fraud are law enforcement agencies, internet security agencies, academia, internet service providers, domain registrars, policy makers, researchers and (last but not the least) the victims. Some of the measures these stakeholders can take to protect themselves and turn the tide against fraudsters .

Internet fraud has been considered a potential cyber threat to the world due to the substantial financial losses victims experience. Thailand is one of the most vulnerable targets of online fraud with the increasing rates of internet users. However, law enforcement seems to inadequately respond to cyber fraud incidents in Thailand.

USER STORY-USER DESCRIPTION:

USER STORY:

Real scam victims have shared their experiences to help warn others about scams.

False billing: John updated supplier details and it ended up costing thousands. You need to have a clearly defined process for verifying and paying accounts and invoices to protect your business against false billing scams.

Travel prize scam: The holiday prize which nearly cost Nicole thousands of dollars. Calls, emails and other approaches claiming that you have won an unexpected prize or a competition you did not enter are almost always scams.

Inheritance scam: Leo gives away his life savings trying to gain an inheritance. Inheritance scams can be quite elaborate to convince you that a fortune awaits. Remember there are no get-rich-quick schemes: if it sounds too good to be true it probably is.

Unexpected prize & lottery scam: Davin's fictional Facebook lottery win. Don't let scammers win the ultimate lottery by gaining your personal details and money. Scammers are highly skilled at deceiving their victims, and may even impersonate someone you know.

Betting & sports investment schemes: Adam's taken for a ride on a horse betting scam

Australians love a bet and sports betting scammers are quick to capitalise on this. They will say anything to draw you in

APPROPOIATE PROCESS FOR FRAUD DETECTION :

- 1) FRAUD SCORING
- 2) 3-D SECURE
- 3) MACHINE LEARNING
- 4) FRAUD BLACKLISTS
- 5) BIOMETRICS
- 6) VELOCITY CHECKS
- 7) ADDRESS VERIFICATION
- 8) DEVICE FINGERPRINTING
- 9) PROXY PIERICING
- 10) GEOLOCATION

EXPERIMENT - 3

DATE :	1/2/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

SYSTEM REQUIREMENT :

SOFTWARE REQUIREMENT :

- operating system windows(10,11) or kali linux
- web browser: TOR ,DUCK DUCK GO,SAFARI

HARDWARE REQUIREMENT :

- RAM Minimum 8GB or higher
- HDD: minimum 5000GB
- PROCESSOR : 9TH Generation Intel core i5 Processor

I . FUNCTIONAL REQUIREMENT FOR PREVENTION:

1. User authentication: Implementing strong authentication methods, such as multi-factor authentication, to verify the identity of users before they access sensitive information or perform transactions.
2. Transaction monitoring: Monitoring all transactions in real-time and identifying any suspicious activity using advanced algorithms and machine learning models.
3. Data encryption: Ensuring that all sensitive data, including financial information, is encrypted during transmission and storage to protect it from unauthorized access.
4. Risk assessment: Regularly assessing the risk of fraud and implementing proactive measures to mitigate that risk

5. User education: Providing users with education and training on how to recognize and avoid fraudulent activity.
6. Alerts and notifications: Providing real-time alerts and notifications to users when suspicious activity is detected on their accounts.
7. :Reporting: Providing users with the ability to report suspected fraud and track the status of their report.
8. Compliance: Ensuring compliance with relevant laws, regulations, and industry standards, such as PCI DSS, to protect against fraud.

II . NON-FUNCTIONAL REQUIREMENT FOR PREVENTION:

- 1) Performance: The system should be able to process transactions and detect fraudulent activity quickly and efficiently, even during periods of high demand.
- 2) Scalability: The system should be able to handle increasing volumes of transactions and data as the number of users and transactions grows.
- 3) Reliability: The system should be highly reliable, with minimal downtime and a low rate of false positive alerts.
- 4) Security: The system should be secure, with proper safeguards in place to prevent unauthorized access and data breaches.
- 5) Usability: The system should be easy to use for both administrators and end-users, with a user-friendly interface and clear, concise notifications and alerts.
- 6) Interoperability: The system should be able to integrate with other systems, such as financial management systems, to provide a comprehensive fraud prevention solution.
- 7) Maintainability: The system should be easy to maintain and upgrade, with minimal disruption to normal operations.
- 8) Compliance: The system should meet relevant legal and regulatory requirements, such as data privacy laws, to protect against fraud.

EXPERIMENT – 4

DATE :	8/2/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

PROJECT PLAN :

- Define project scope and objectives: Determine the specific goals and objectives of the project, including the type of fraud to be prevented, the user groups to be protected, and any legal or regulatory requirements that must be met.
- Conduct a risk assessment: Analyze the current state of the system to identify potential security weaknesses and areas of risk.
- Choose a solution: Evaluate different fraud prevention solutions and choose the one that best meets the needs of the organization.
- Plan the implementation: Develop a detailed project plan, including milestones, timelines, and resource requirements.
- Obtain necessary approvals: Obtain approval from stakeholders and any relevant regulatory agencies.
- Set up infrastructure: Prepare the necessary infrastructure, including servers, storage, and networking equipment, to support the fraud prevention solution.
- Install the solution: Install and configure the chosen fraud prevention solution.
- Test and validate: Conduct extensive testing and validation to ensure that the solution is working as expected and meets the objectives of the project.
- Go live: Deploy the solution and begin using it to prevent fraud in real-world transactions.

- **Monitor and maintain:** Monitor the solution on an ongoing basis and perform regular maintenance to ensure that it continues to function effectively and meet the needs of the organization.

ROLES AND RESPONSIBILITIES PREVENTING ONLINE FRAUD :

1. **Project Manager:** The project manager is responsible for overseeing the overall project, including defining project scope and objectives, creating a project plan, and ensuring that the project is completed on time and within budget.
2. **Technical Lead:** The technical lead is responsible for managing the technical aspects of the project, including choosing and installing a fraud prevention solution, configuring and testing the solution, and ensuring that it integrates with other systems.
3. **Security Analyst:** The security analyst is responsible for conducting a risk assessment, identifying areas of vulnerability, and recommending security controls to prevent fraud.
4. **User Trainer:** The user trainer is responsible for providing training to users on how to use the fraud prevention solution and how to recognize and avoid fraudulent activity.
5. **Support Team:** The support team is responsible for providing ongoing technical support and maintenance for the fraud prevention solution, including troubleshooting issues and addressing user questions.
6. **Compliance Officer:** The compliance officer is responsible for ensuring that the fraud prevention solution complies with relevant laws, regulations, and industry standards, such as data privacy laws and PCI DSS.
7. **Management:** Senior management is responsible for providing support and resources for the project and for setting the overall direction for the organization's fraud prevention efforts.

NAME	ROLES
N SAI SADWIK REDDY	<ul style="list-style-type: none"> • SUBJECT MATTER EXPERT • SOFTWARE DEVELOPER • PROJECT OWNER
SHIVNATH CHIRANJEEVI	<ul style="list-style-type: none"> • SUBJECT MATTER EXPERT • PROJECT MANAGER • TECHNICAL LEAD • PROJECT OWNER
K VENKATA RAMA SUJAL	<ul style="list-style-type: none"> • PROJECT SPONSOR • SOFTWARE TESTER • PROJECT OWNER

EXPERIMENT – 5

DATE :	15/2/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

WORK BREAKDOWN STRUCTURE (WBS) :

A Work Breakdown Structure (WBS) is a hierarchical decomposition of a project into smaller, more manageable components. In the context of online fraud detection, a typical WBS might include the following elements:

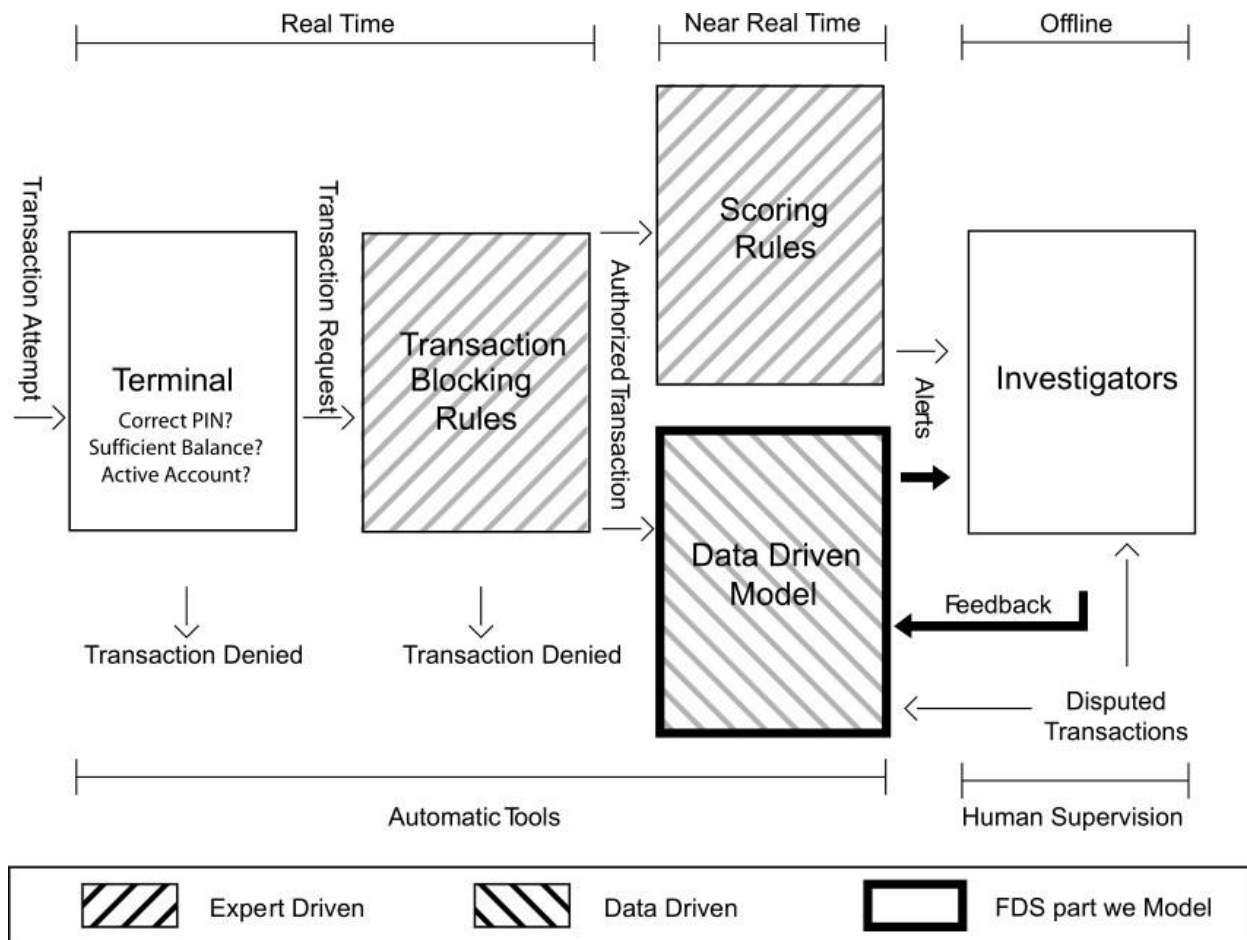
Planning: Define the project scope, objectives, and constraints, as well as the approach for detecting online fraud.

Data collection and preparation: Gather and clean the data needed for fraud detection, such as transaction data, customer information, and previous fraud cases.

Feature engineering: Engineer relevant features from the data to be used for the detection of online fraud.

Model development: Develop, test, and evaluate various fraud detection models using the prepared data and features.

Model deployment: Deploy the selected model in the production environment, monitor its performance, and make any necessary updates or improvements.



SIZE ESTIMATION TECHNIQUES :

Size estimation techniques are used to determine the resources required to complete a project or a task. In the context of online fraud detection, size estimation can help to determine the amount of effort required to develop and deploy a fraud detection system. The following are some of the commonly used size estimation techniques in online fraud detection:

Function Point Analysis (FPA): FPA is a technique that measures the functionality provided by a software system. In the context of online

fraud detection, FPA can be used to determine the size of the system in terms of the number of transactions it can process and the number of fraud cases it can detect.

Use Case Points (UCP): UCP is a technique that measures the size of a software system based on the number and complexity of use cases.

In online fraud detection, UCP can be used to estimate the size of the system in terms of the number of fraud scenarios it can handle.

Story Points: Story points are a measure of the relative size and complexity of a software feature or user story. In online fraud detection, story points can be used to estimate the size of individual components of the system, such as data preparation, feature engineering, or model deployment.

Expert judgment: Expert judgment is a technique where experienced professionals are asked to provide their estimate of the size of a project based on their knowledge and experience. In online fraud detection, expert judgment can be used to estimate the size of the system based on the complexity of the data and the algorithms used for fraud detection.

These are just a few examples of size estimation techniques that can be used in online fraud detection. The choice of technique depends on the specific requirements and complexities of the project, as well as the available resources and expertise.

DEPENDENCY GRAPH :

A dependency graph is a visual representation of the relationships between tasks or activities in a project. In the context of online fraud detection, a dependency graph can be used to understand the interdependencies between different components of the system and

to identify critical paths and potential bottlenecks in the development and deployment process.

A typical dependency graph for online fraud detection might include the following elements:

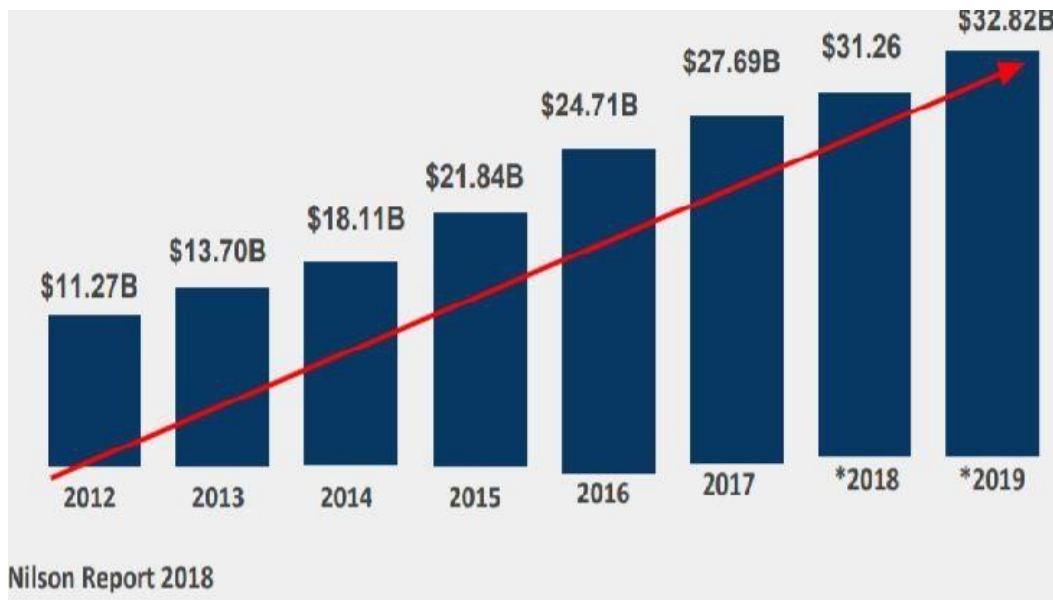
Data collection and preparation: This is usually the first step in the online fraud detection process and is dependent on the availability of relevant data.

Feature engineering: This step depends on the data collected and prepared in the previous step and involves creating relevant features from the data that will be used for fraud detection.

Model development: This step depends on the engineered features and involves developing and testing various fraud detection models.

Model deployment: This step depends on the successful completion of the previous steps and involves deploying the selected model in the production environment.

DEPENDENCY GRAPH GIVEN BELOW :



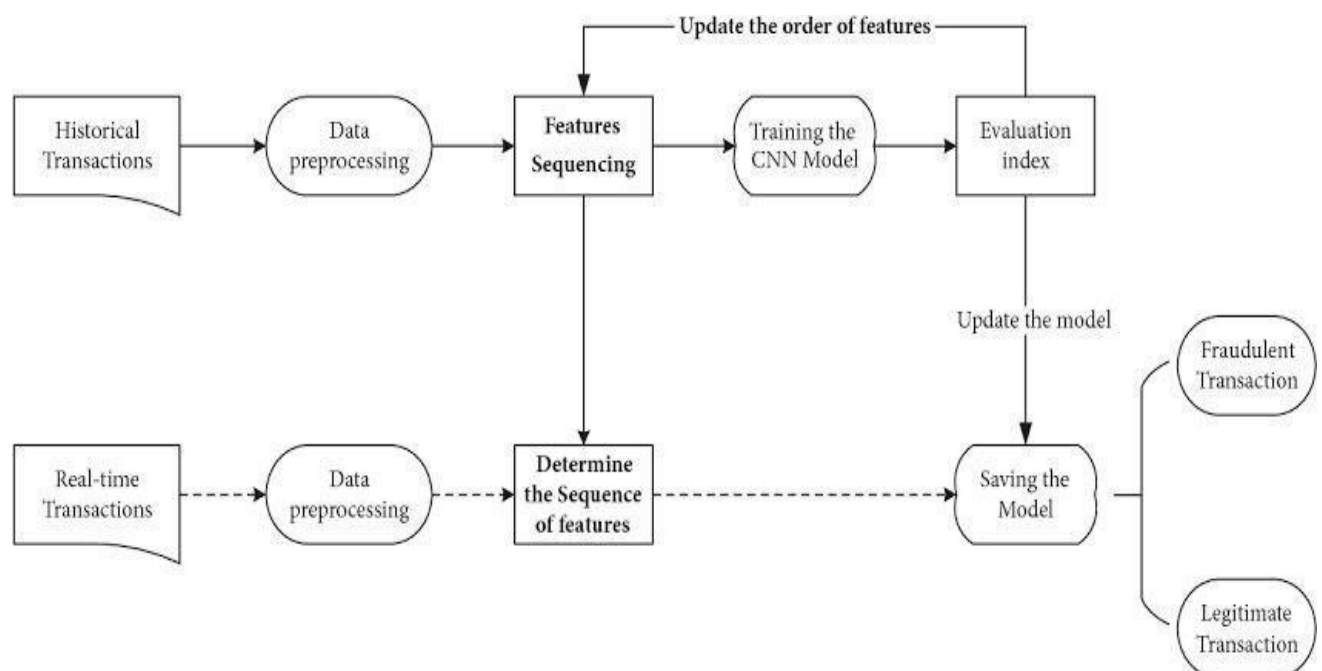
NETWORK DIAGRAM :

A network diagram is a visual representation of the activities and dependencies in a project. In the context of online fraud detection, a network diagram can be used to illustrate the steps involved in the process, the interdependencies between those steps, and the critical paths that need to be completed in a timely manner.

A typical network diagram for online fraud detection might include the following elements:

Data collection and preparation: This is usually the first step in the online fraud detection process and involves collecting and cleaning the data needed for the analysis.

EXAMPLE OF NETWORK DIAGRAM GIVEN BELOW :



TIMELINE :

A timeline is a visual representation of the planned and actual progress of a project over time. In the context of online fraud detection, a timeline can be used to outline the key milestones and activities involved in the process, as well as to track the progress of the project against the schedule.

A typical timeline for online fraud detection might include the following milestones:

Data collection and preparation: This is usually the first step in the online fraud detection process and involves collecting and cleaning the data needed for the analysis.

Feature engineering: This step involves creating relevant features from the data that will be used for fraud detection.

Model development: This step involves developing and testing various fraud detection models.

Model deployment: This step involves deploying the selected model in the production environment.

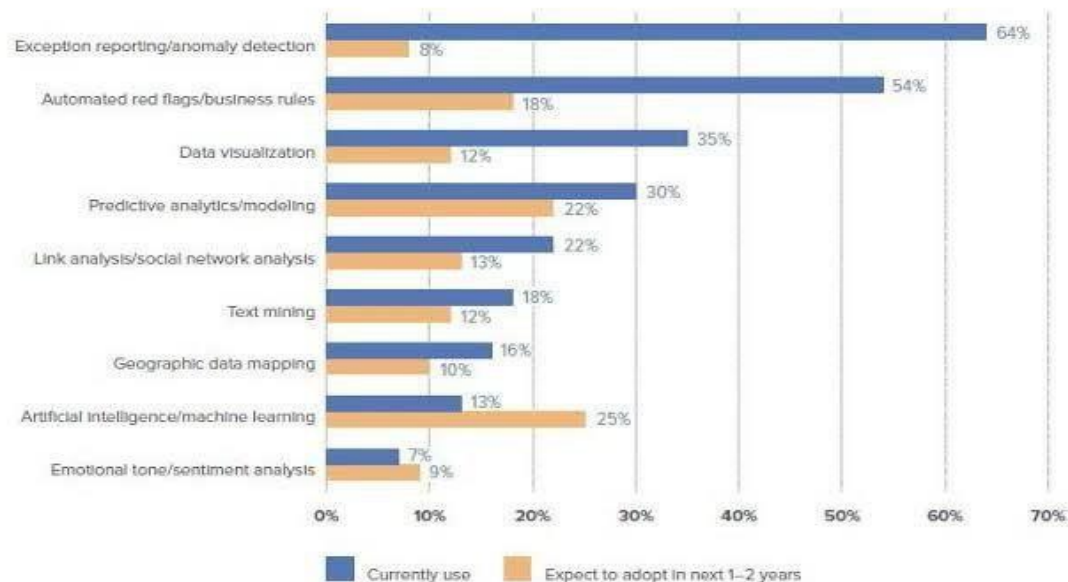
Fraud investigation and resolution: This step involves investigating and resolving any detected fraud cases.

Evaluation and reporting: This step involves evaluating the performance of the fraud detection system and documenting the results.

These milestones can be represented on the timeline as horizontal bars that extend over the duration of the project. The timeline can also include intermediate steps or activities that are necessary to complete the project, such as testing and debugging.

EXAMPLE OF CHART IN ONLINE FRAUD :

FIG. 1 What data analysis techniques do organizations use to fight fraud?



RISK ANALYSIS :

Risk analysis is the process of identifying and evaluating potential risks associated with a project or system. In the context of online fraud detection, risk analysis is used to identify potential risks that could impact the effectiveness or reliability of the system and to develop mitigation strategies to reduce or eliminate those risks.

A typical risk analysis for online fraud detection might include the following steps:

Identify potential risks: This step involves identifying all the potential risks associated with the online fraud detection system, such as data quality issues, system malfunctions, or false positive alerts.

Evaluate the risks: This step involves evaluating the likelihood and impact of each potential risk, as well as the effectiveness of existing mitigation strategies.

Develop mitigation strategies: This step involves developing and implementing strategies to reduce or eliminate the risks identified in the previous steps. These strategies could include additional testing and quality control measures, or the development of backup systems to ensure continuity of service.

Monitor and review: This step involves continuously monitoring the online fraud detection system for potential risks and reviewing the risk analysis on a regular basis to ensure that it remains relevant and up-to-date.

By conducting a risk analysis for online fraud detection, project managers can ensure that the system is designed and implemented in a way that minimizes the risk of fraud and maximizes the reliability of the system. This can help to improve the overall effectiveness of the online fraud detection system and increase confidence in its results.

SWOT ANALYSIS :

Strengths :

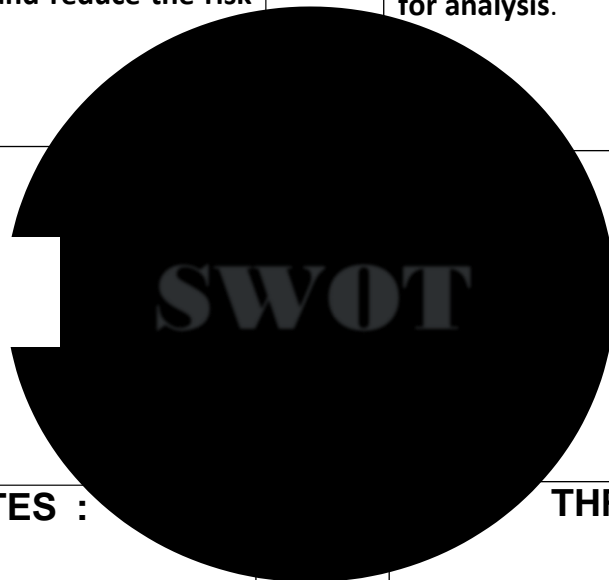
Advanced technologies: The use of advanced technologies such as machine learning and artificial intelligence can greatly improve the accuracy and speed of fraud detection.

Real-time monitoring: The ability to monitor transactions in real-time can help to detect fraud quickly and reduce the risk of financial losses.

WEAKNESS :

False positives: The risk of false positives can lead to a high number of false alerts and increase the workload of investigators.

Dependence on data quality: The accuracy of the fraud detection system can be impacted by the quality of the data used for analysis.



OPPURTUNITES :

Increased use of online transactions: The increasing use of online transactions provides a growing opportunity for fraud detection systems to detect and prevent fraud. **Improved customer experience:** A successful fraud detection system can help to improve customer experience by reducing the risk of fraud and increasing confidence in online transactions.

THREATS :

Cyber attacks: The risk of cyber attacks, such as hacking and phishing, can pose a significant threat to the effectiveness of fraud detection systems.

RISK MITIGATION :

RESPONSE	STRATEGY	EXAMPLES
AVOID	Monitoring the data which feeds, trains and tests the model. Avoiding fake account. Keeping backup servers.	Web scraping for data Fake bookings. Server breakdown.
TRANSFER	Clearly stating out the accessed policies and risks, especially concerning the data and model usage, for the transference to the third party	Proper statement for the transfer of data from the doctor to patient and vice versa.
MITIGATE	One important strategy for the mitigation of all the major potential threats, includes the prior through study	Exploration of all the data sources and data-points and its careful analysis
ACCEPT	Putting down all the achievable endpoints and non-achievable deadends, during the course of prior dealings.	Scenario planning for tackling situations in a planned fashion.

EXPERIMENT – 6

DATE :	22/2/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

COCOMO MODEL :

COCOMO is one of the most widely used software estimation models in the world. This model is developed in 1981 by Barry Boehm to give an estimate of the number of man-months it will take to develop a software product. COCOMO predicts the efforts and schedule of a software product based on size of the software. COCOMO stands for Constructive Cost Model.

COCOMO has three different models that reflect the complexity

- Basic model
- Intermediate model
- Detailed model

Similarly there are three classes of software projects.

- 1) **Organic mode** :- In this mode, relatively small, simple software projects with a small team are handled. Such a team should have good application experiences to less rigid requirements.
- 2) **Semi-detached Projects** :- In this class an intermediate projects in which teams with mixed experience level are handled. Such projects may have mix of rigid and less than rigid requirements.

3) **Embedded Project** :- In this class, projects with tight hardware, software and operational constraints are handled.

Let us understand each model in detail.

I) **Basic Model** The basic CCWOMO model estimates the software development effort using only Lines Of Code (LOC). Various equations in this model are —

$$E = a_b (KLOC)^{b_b}$$

$$D = C_b (E)^{d_b}$$

$$P = E/D$$

Where E is the effort applied in person- months.

D is the development time in chronological months.

KLOC means kilo line Of code for the project.

P is the total number Of persons required to accomplish the

The coefficient of these a_b , b_b , c_b , d_b three modes are as given below.

Software Projects	a_b	b_b	c_b	d_b
Organic	2.4	1.05	2.5	0.38
Semi- detached	3.0	1.12	2.5	0.35
Embedded	3.6	1.20	2.5	0.32

Merits or Basic COCOMO :

1. Basic COCOMO model is good for quick, early, rough order of magnitude estimate of software project.

Limitations of Basic :

The accuracy Of this model is limited because it does not consider certain factors for

cost of software, these are hardware constraints, ad quality, and experience, modern and tools.

The estimate of COCOMO model are within a factor of 1.3 only 29% Of the time and within the factor Of 2 only 60% Of time.

EXPERIMENT – 7

DATE :	1/3/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

SYSTEM DESIGN ARCHITECTURE :

Fraud detection is a set of activities that are taken to prevent money or property from being obtained through false pretenses.”Fraud can be committed in different ways and in many industries. Credit card frauds are easy and friendly targets. E- commerce and many other online sites have increased the online payment modes, increasing the risk for online frauds.

Increase in fraud rates, researchers started using different machine learning methods to detect and analyse frauds in online transactions. Credit card fraud generally happens when the card was stolen for any of the unauthorized purposes or even when the fraudster uses the credit card information for his use. Lots of money are lost due to credit card fraud every year.

There is a lack of research studies on analyzing real-world credit card data owing to confidentiality issues. In this paper, machine learning algorithms are used to detect credit card fraud. To evaluate the model efficacy, a publicly available credit card data set is used. The System prediction level & accuracy of fraud detection is not 100 percent accurate, So there is a chance of getting fraud.

Then, a real-world credit card data set from a financial institution is analyzed. In addition, noise is added to the data samples to further assess the robustness of the algorithms. The experimental results positively indicate that the majority voting method achieves good accuracy rates in detecting fraud cases in credit cards.

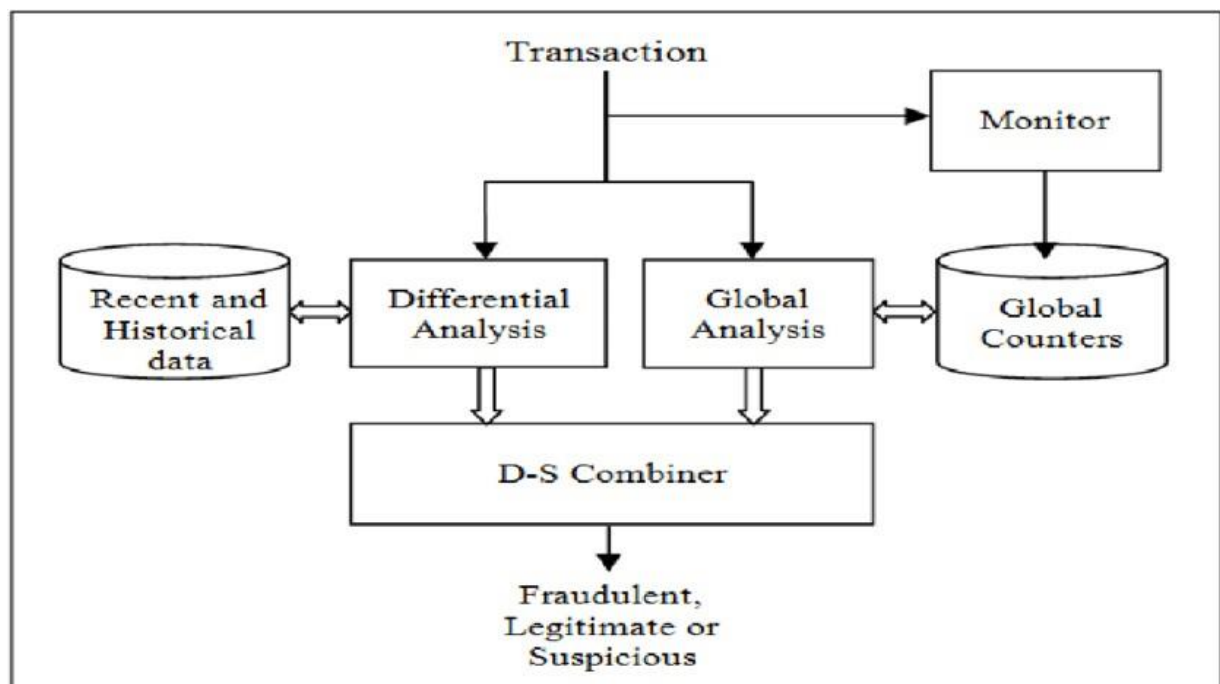


Fig. Block diagram for Online Fraud Detection.

Our Project main purpose is to making Credit Card Fraud Detection awaring to people from credit card online frauds. the main point of credit card fraud detection system is necessary to safe our transactions & security. With this system, fraudsters don't have the chance to make multiple transactions on a stolen or counterfeit card before the cardholder is aware of the fraudulent activity. This model is then used to identify whether a new transaction is fraudulent or not. Our aim here is to detect 100% of the fraudulent transactions while minimizing the incorrect fraud classifications.

The following diagram shows the complete System Architecture :

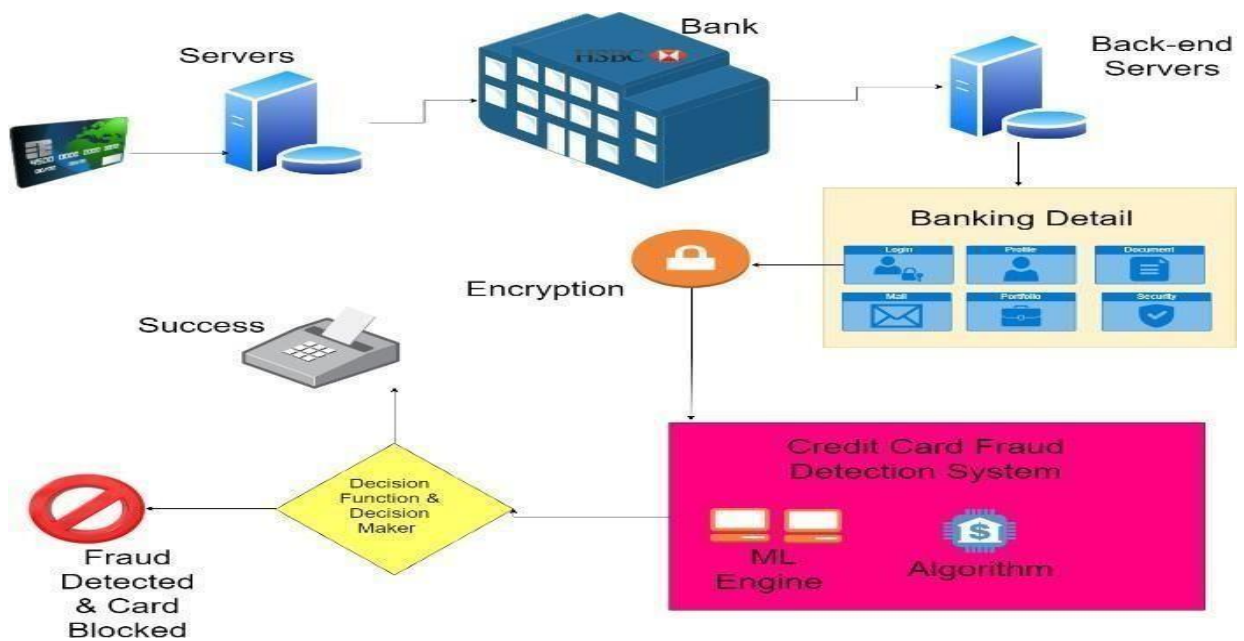
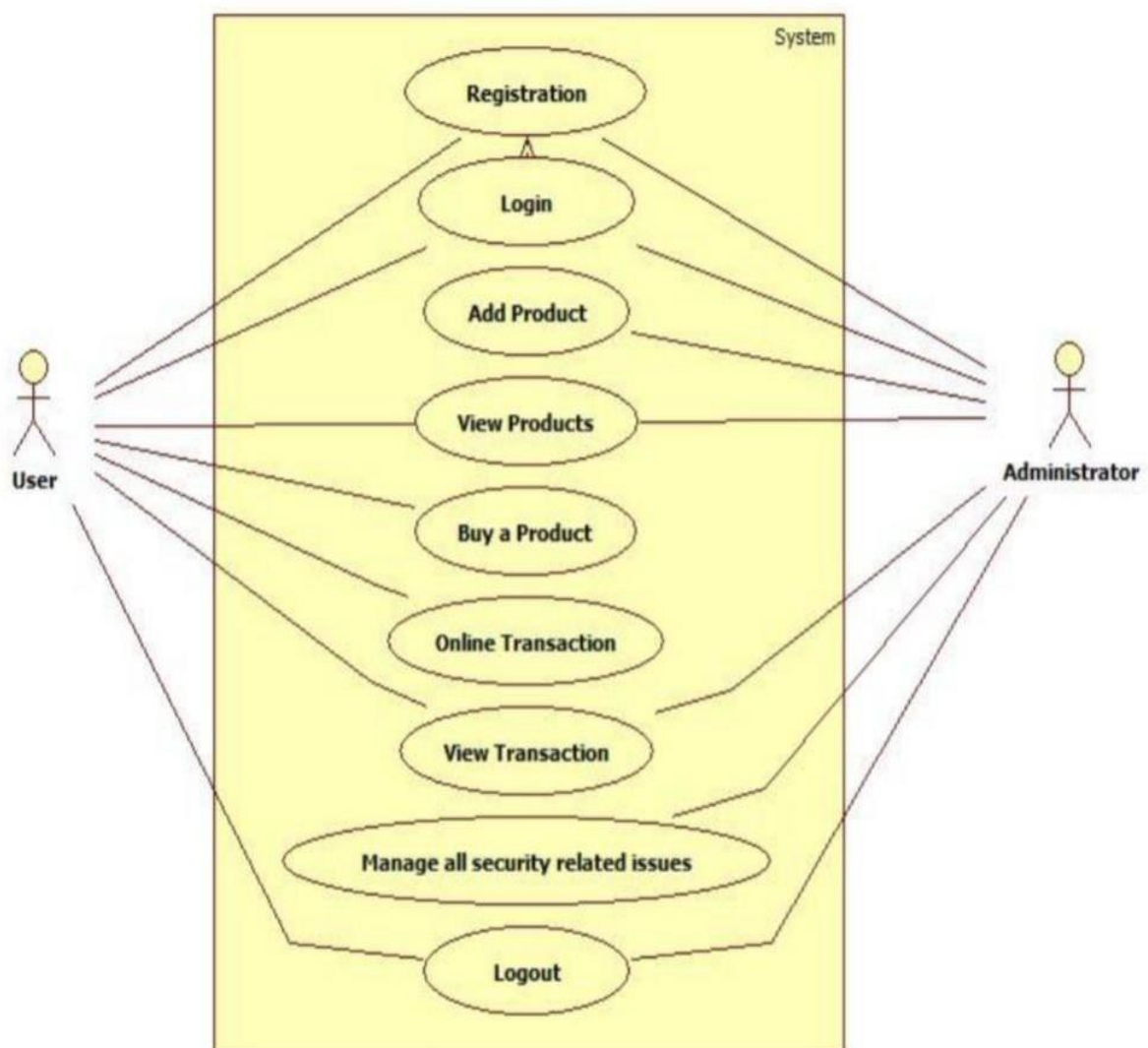


Fig. System Architecture Diagram

EXPERIMENT – 8

DATE :	8/3/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

USE CASE DIAGRAM :



1. Admin :

- a. Login : Admin need to login using valid login credentials in order to access the system.
- b. Add / View Products : Admin can add new product with its details into the system.
- c. View Transactions : System allows admin to view all the transactions done by the registered users.

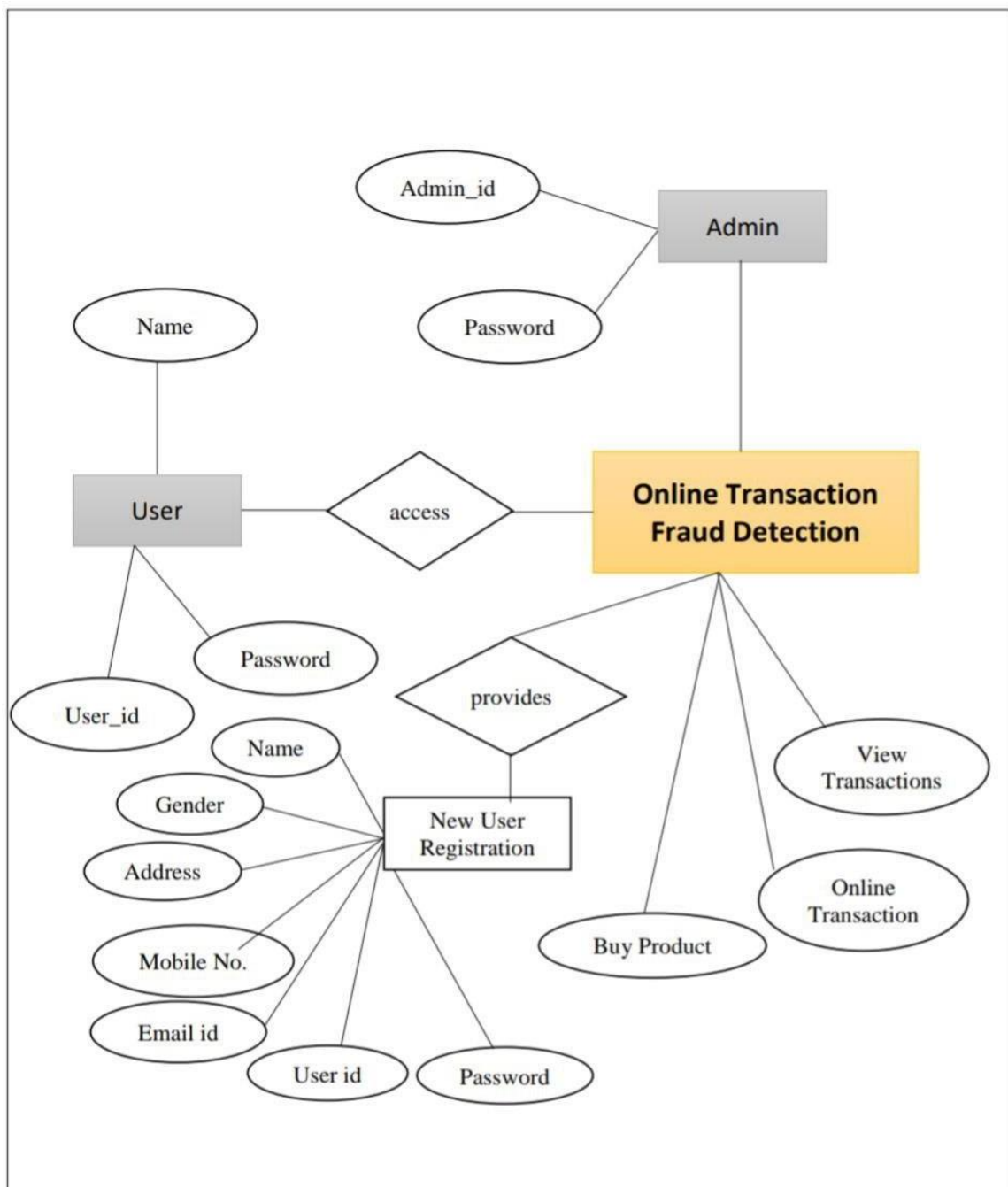
2. User :

- a. Registration : Here, user first need to registration themselves with details to access the system.
- b. Login : After a successful registration, user then need to login into the system by inputting their credentials into the system.
- c. View Products : User can view multiple products with its details. Interested users can purchase a product via online transaction.
- d. Buy a Product : User can select payment mode to perform transactions by providing the card details like card no., CVV code, Expiry Date and Holders name.
- e. View Transaction : List of all the transactions will be displayed to the user.

EXPERIMENT -9

DATE :	15/3/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

ENTITY RELATIONSHIP DIAGRAM :



Attributes of Entity :

Most existing fraud detection research presumes the existence of labeled data and reliability of these labels and emphasizes ML techniques to better predict fraud. To the best of our knowledge, DeFraudNet is the first end-to-end system that combines label generation to model serving in a unified framework. Our system consists of 4 stages .

1. Data and feature pipeline : This is responsible for building the features that go into the training, validation and ‘golden’ datasets.
2. Label generation pipeline : This contains the components to generate weak labels for all data points in the training and validation datasets.
3. Discriminator pipeline : This trains the final discriminator models on features and labels from the previous stages.
4. Evaluation : This facilitates ongoing evaluation of the fraud detection system by sending a sample of claims to human evaluators and using their judgment to compute precision, recall and related health-check metrics.

Data And Feature Processing :

Initially the dataset consists of all unclassified claims U . A small random sample from U is sent to the Risk Management Team (RMT) which manually adjudicates cases to generate ‘strong’ labels. We call this the ‘golden’ dataset G . This dataset is inherently expensive and slow to generate (a few hundred labels).

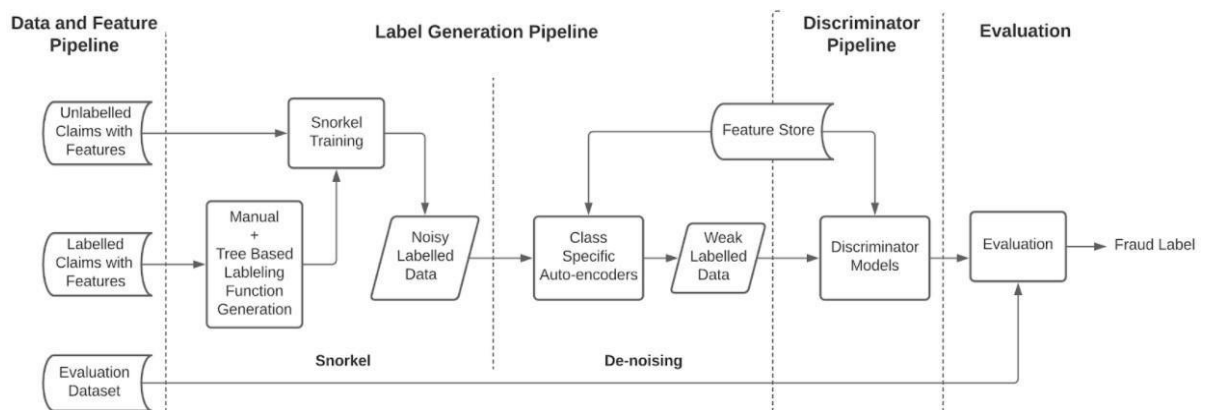


Fig.1. DeFraudNet End to End Framework

EXPERIMENT – 10

DATE :	22/3/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

DOMAIN CLASS :

The frequency domain representation allows us to perform a transaction analysis in terms of the magnitude assumed by each frequency component that characterizes the transaction, allowing us to detect some patterns in the features that are not discoverable otherwise. As preliminary work, we compared the two different representation of a transaction (i.e., these obtained in the time and frequency domains), observing some interesting properties for the context taken into account in this paper, which are described in the following :

1. User: This class represents a user who interacts with an online system. It includes attributes such as user ID, name, address, email, and phone number.
2. Transaction: This class represents a transaction made by a user in the online system. It includes attributes such as transaction ID, date, time, amount, and status.
3. Payment Method: This class represents the payment method used by a user to make a transaction. It includes attributes such as payment method ID, name, type, and account details.

4. **Fraud Detection System:** This class represents the system used to detect fraud in online transactions. It includes attributes such as detection rules, algorithms, and thresholds.
5. **Risk Assessment:** This class represents the assessment of the risk associated with a transaction. It includes attributes such as risk score, risk level, and risk factors.
6. **Alert:** This class represents an alert generated by the fraud detection system when a transaction is deemed to be high risk. It includes attributes such as alert ID, date, time, and reason.
7. **Investigation:** This class represents the investigation of a high-risk transaction. It includes attributes such as investigator ID, date, time, and outcome.
8. **Resolution:** This class represents the resolution of a high-risk transaction. It includes attributes such as resolution ID, date, time, and outcome.
9. Overall, the domain class for online fraud detection includes classes that represent users, transactions, payment methods, the fraud detection system, risk assessment, alerts, investigations, and resolutions. These classes work together to prevent and detect fraudulent activities in online transactions.

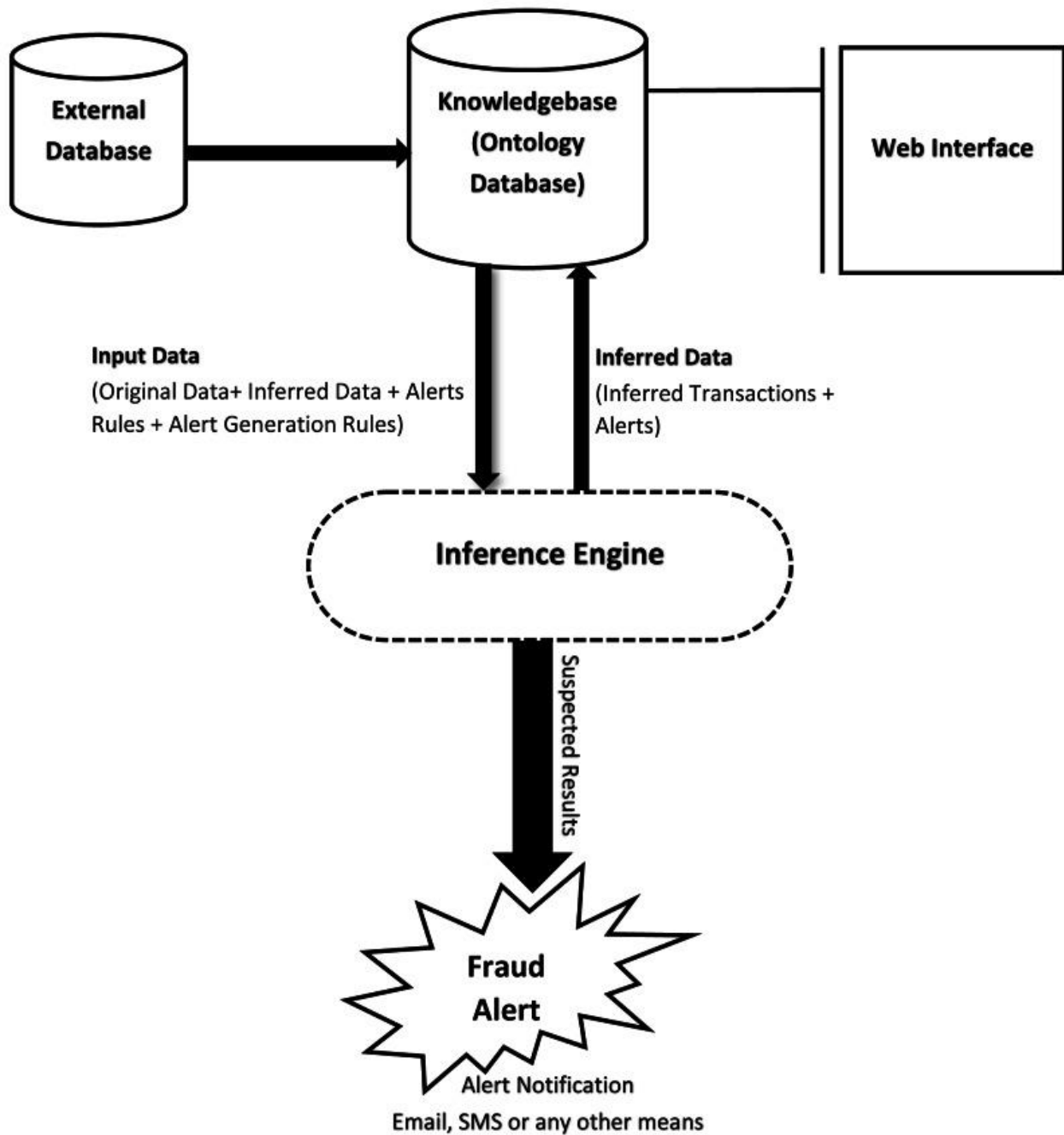
USER GENERALIZATION :

Generalization is a technique in data modeling that involves creating a higher-level entity to represent a set of lower-level entities. In the context of online fraud detection, generalization can be used to create a higher-level entity that represents a group of transactions that share similar characteristics. By creating such an entity, we can apply fraud detection rules and algorithms to the group as a whole, instead of analyzing each transaction individually.

For example, we can create a higher-level entity called "High-Risk Transactions" that represents transactions that exhibit one or more high-risk characteristics. These characteristics may include large transaction amounts, unusual transaction patterns, suspicious IP addresses or devices, and so on. By generalizing these transactions, we can apply fraud detection algorithms to the group as a whole, such as machine learning models that have been trained on historical data.

In summary, generalization can be a useful technique in online fraud detection as it allows us to apply fraud detection algorithms to a group of entities that share similar characteristics, rather than analyzing each entity individually. This can help to improve the efficiency and effectiveness of fraud detection systems.

USING SUBCLASSES :



Subclasses are a technique in object-oriented programming that involves creating a specialized class that inherits attributes and methods from a more general class. In the context of online fraud detection, subclasses can be used to create specialized classes that represent specific types of transactions, users, or payment methods that exhibit high-risk characteristics. By creating such subclasses, we can apply specialized fraud detection rules and algorithms that are tailored to these specific types of entities.

For example, we can create a subclass called "Credit Card Transactions" that inherits from the more general "Transactions" class. This subclass can include specialized fraud detection rules and algorithms that are specific to credit card transactions, such as checking for large transactions made outside of the user's usual spending patterns, checking for transactions made from unusual locations or devices, or checking for multiple transactions made in a short period of time. By using specialized rules and algorithms for credit card transactions, we can improve the accuracy of fraud detection for this specific type of transaction.

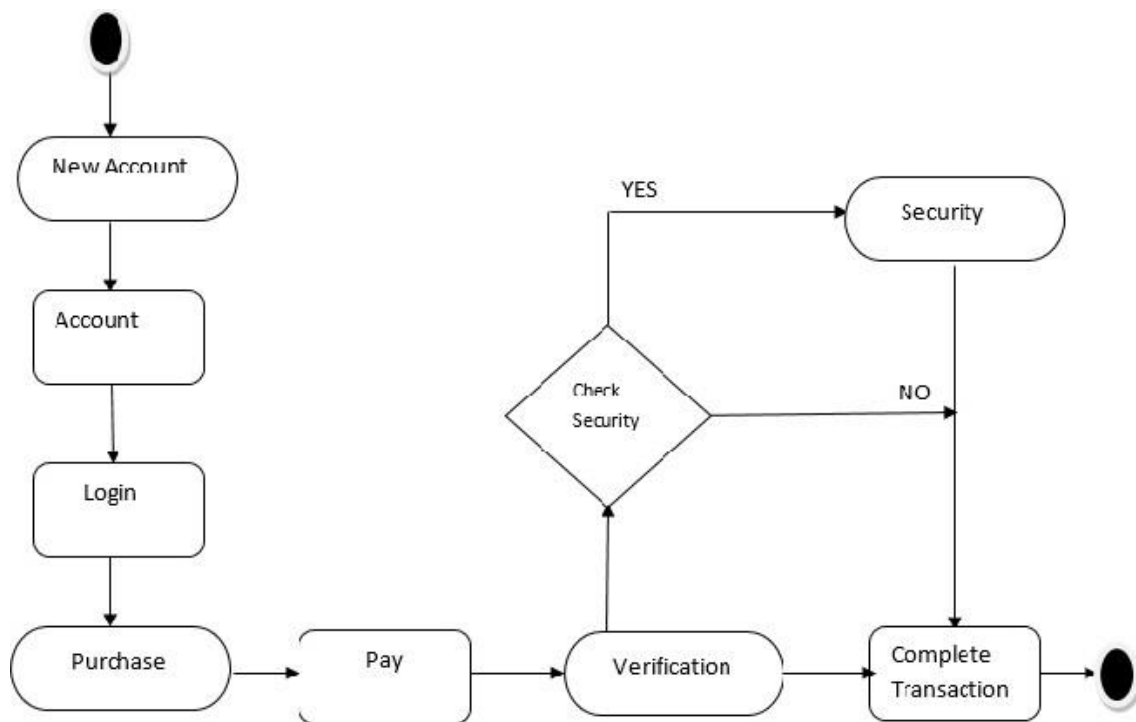
Subclasses can also be used for payment methods, such as creating a subclass for "Prepaid Cards" or "Virtual Credit Cards". These subclasses can include specialized fraud detection rules and algorithms that are specific to these payment methods, such as monitoring for a high number of transactions made with the same prepaid card or virtual credit card.

In summary, subclasses can be a useful technique in online fraud detection as they allow for the creation of specialized classes that can apply specialized fraud detection rules and algorithms to specific types of transactions, users, or payment methods. This can improve the accuracy of fraud detection by tailoring the rules and algorithms to the specific characteristics of these entities.

EXPERIMENT – 11

DATE :	29/3/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

STATECHART DIAGRAM :



There are several different methods that can be used for online fraud detection, including:

1. Transaction monitoring: This involves analyzing transactional data in real-time to identify patterns or anomalies that may indicate fraud.

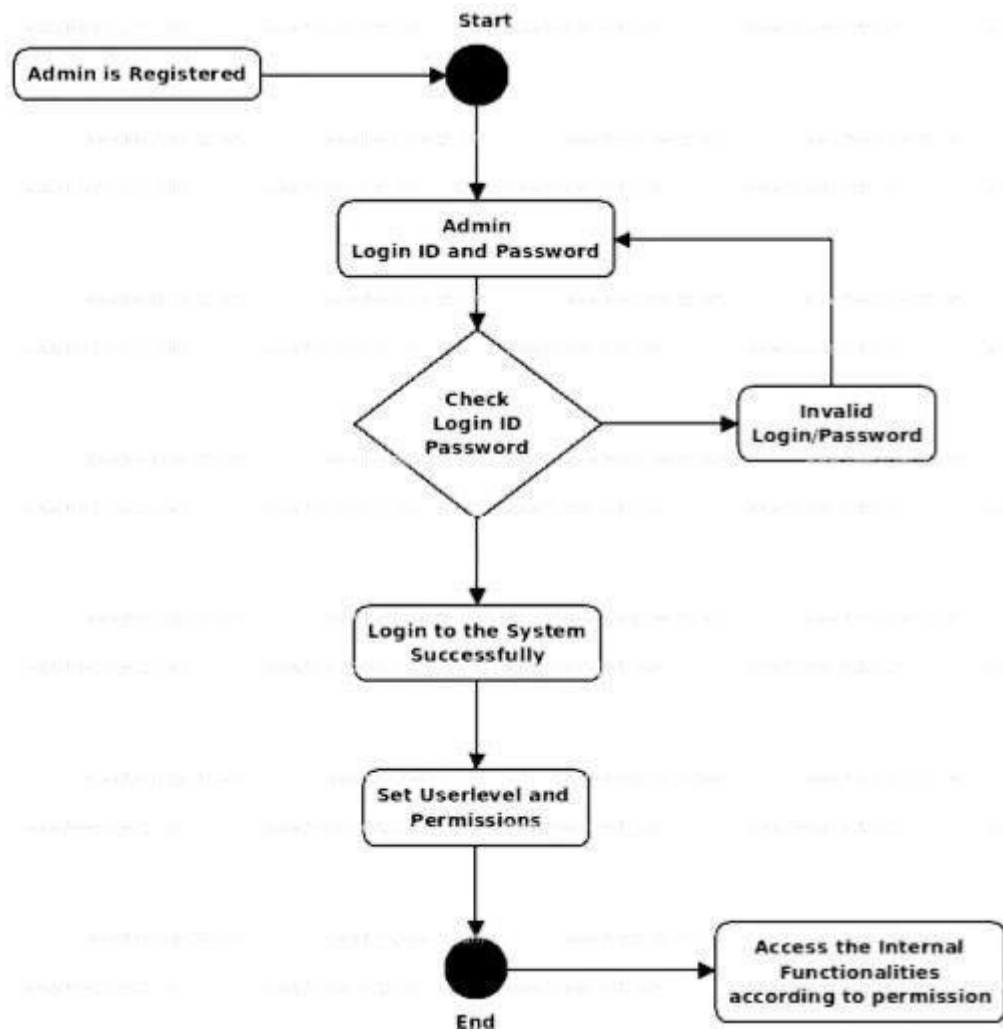
2. Machine learning algorithms: These are used to analyze large amounts of data and identify patterns that may be indicative of fraudulent behavior.
3. Behavioral analytics: This involves analyzing user behavior over time to identify patterns that may indicate fraudulent activity.
4. Biometric authentication: This involves using physical characteristics like fingerprints or facial recognition to verify the identity of users and prevent fraud.
5. Two-factor authentication: This involves requiring users to provide two forms of identification (such as a password and a security token) in order to access their accounts, which can help prevent fraud.

TRANSITION :

The field of online fraud detection has undergone significant transitions in recent years, as new technologies and approaches have emerged to help organizations stay ahead of evolving threats. Here are some of the key transitions in the field:

- i. From rule-based to machine learning-based approaches: In the past, many online fraud detection systems relied on pre-defined rules to identify suspicious activity. However, with the advent of machine learning and artificial intelligence, many systems now use algorithms that can learn from large datasets and adapt to new types of fraud.
- ii. From reactive to proactive detection: Many online fraud detection systems are now designed to detect suspicious activity in real-time, allowing organizations to take proactive measures to prevent fraud before it occurs. This is a departure from traditional reactive approaches, which were focused on detecting fraud after the fact.

ACTIVITY DIAGRAM :



COMPONENTS OF AN ACTIVITY DIAGRAM :

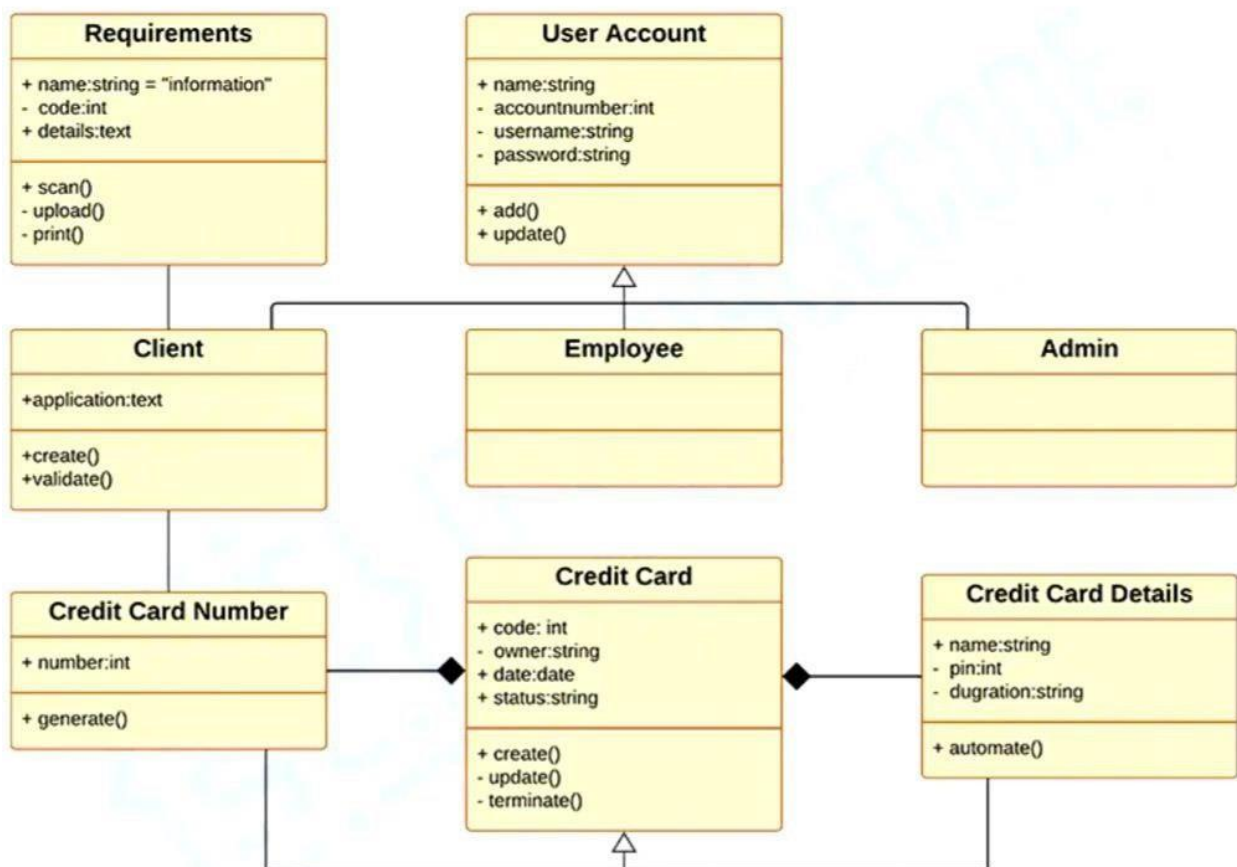
- **Initial Node:** The initial node represents the starting point of the activity diagram, where the process or use case begins.
- **Action/Activity:** An action or activity is a specific task or operation that is performed within the process or use case. It is represented by a rectangular box with rounded corners, and its name is written inside the box.
- **Decision Node:** The decision node is used to represent a decision point in the process, where the flow of activities may take different paths based on a certain condition or criteria. It is represented by a diamond-shaped box.
- **Merge Node:** The merge node is used to merge multiple paths or branches in the process back into a single path. It is represented by a diamond-shaped box with a plus sign in the center.
- **Fork Node:** The fork node is used to split the process into multiple parallel paths or branches. It is represented by a horizontal line with multiple lines branching out from it.
- **Join Node:** The join node is used to rejoin multiple parallel paths or branches back into a single path. It is represented by a horizontal line with multiple lines merging into it.
- **Final Node:** The final node represents the end of the process or use case, where the process is complete. It is represented by a circle with a solid border.

These components can be used to create a visual representation of the flow of activities in a process or use case, which can help stakeholders to better understand the process and identify potential areas for improvement or optimization.

EXPERIMENT – 12

DATE :	30/3/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

CLASS DIAGRAM :



CLASS :

In the context of online fraud detection, a class can refer to a category or label assigned to a transaction or event based on its characteristics or risk level. Classes can be used to group transactions or events based on their attributes, such as the amount, location, type of transaction, user behavior, and so on.

For example, a fraud detection system might assign different classes to transactions based on their level of risk, such as low-risk, medium-risk, or high-risk. Each class may have a different set of rules or criteria for determining fraud, such as transaction amount thresholds, geographic location, or user behavior patterns.

RELATIONSHIPS :

In the context of online fraud detection, relationships refer to the connections or dependencies between various entities or factors that contribute to the occurrence of fraud. These relationships can be analyzed and modeled to better understand the underlying patterns and dynamics of fraud, and to develop more effective strategies for detecting and preventing it.

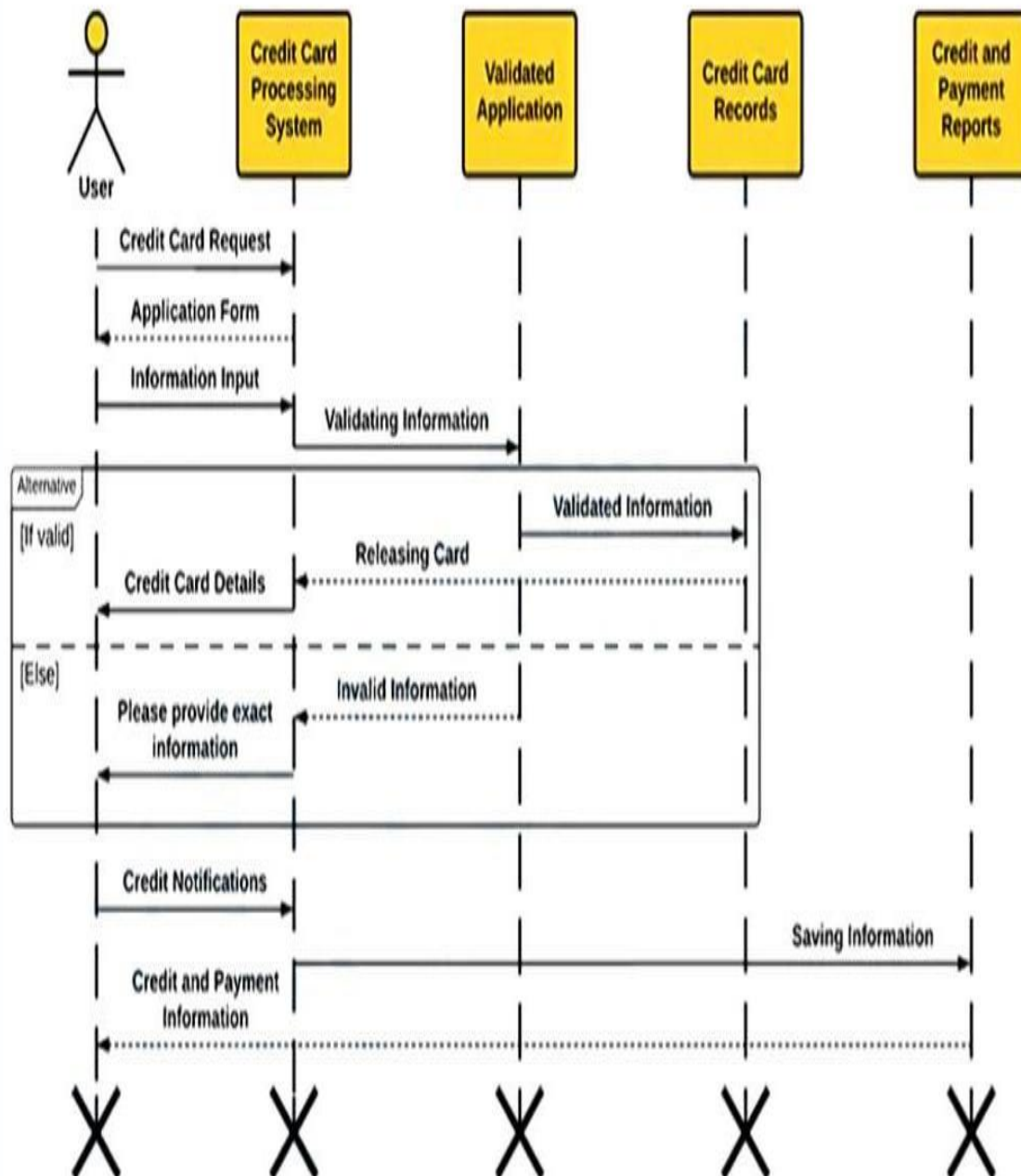
Some examples of relationships in online fraud detection include:

1. User behavior: The behavior patterns of users, such as their browsing history, transaction history, and geographic location, can be analyzed to detect anomalies or patterns that are indicative of fraud.

2. Transaction history: The history of transactions associated with a particular account or user can be analyzed to identify suspicious patterns or activity, such as sudden increases in transaction volume, or frequent transactions to unusual locations.
3. Network connections: The connections between different entities involved in a transaction, such as the user, the merchant, and the payment processor, can be analyzed to identify suspicious relationships or dependencies that may be indicative of fraud.
4. Device information: The characteristics and history of the device used to initiate a transaction, such as the IP address, browser version, and operating system, can be analyzed to detect anomalies or patterns that may be indicative of fraud.
5. Risk factors: The various risk factors associated with a transaction, such as the transaction amount, type of merchandise, and delivery location, can be analyzed to identify patterns and dependencies that may be indicative of fraud.

Overall, analyzing and modeling relationships in online fraud detection can provide valuable insights into the underlying patterns and dynamics of fraud, and can help to develop more effective strategies for detecting and preventing it.

SEQUENCE DIAGRAM :



OBJECT :

An object can refer to any entity or item that is involved in a transaction or event that is being analyzed for fraud. Objects can be anything from a user account, to a payment card, to a device or browser used to initiate a transaction.

Objects can be analyzed in various ways to detect patterns or anomalies that may indicate fraud. For example:

- **User objects:** User objects refer to the user accounts associated with a transaction or event. User objects can be analyzed to detect anomalies in user behavior, such as sudden changes in transaction volume, unusual login locations, or patterns of behavior that deviate from typical usage.
- **Payment objects:** Payment objects refer to any item or entity involved in a payment transaction, such as a payment card, a bank account, or a payment processor. Payment objects can be analyzed to detect anomalies in payment activity, such as transactions that are larger than typical, transactions that occur at unusual times or locations, or transactions that involve multiple payment methods.
- **Device objects:** Device objects refer to the devices or browsers used to initiate a transaction or event. Device objects can be analyzed to detect anomalies in device behavior, such as patterns of device usage that differ from typical behavior, or devices that are associated with known fraud or malware.

Overall, analyzing objects is an important part of online fraud detection, as it allows for the identification of patterns and anomalies that may indicate fraudulent activity. By analyzing the behavior and characteristics of objects involved in a transaction or event, fraud detection systems can help to detect and prevent fraud in real-time.

LIFE-LINE BAR :

In the context of online fraud detection, a lifeline bar is a graphical element used in sequence diagrams or activity diagrams to represent the lifespan of an object or entity involved in a transaction or event. A lifeline bar typically consists of a vertical line representing the object's lifespan, with horizontal bars or notches indicating specific events or actions that occur during the object's lifespan.

A lifeline bar may be used to represent the lifespan of an object such as a user account, a payment card, or a device used to initiate a transaction. The horizontal bars or notches on the lifeline bar can represent specific events or actions that occur during the object's lifespan, such as login attempts, payment transactions, or suspicious activity alerts.

Lifeline bars are useful for visualizing the flow of events and actions in a system, and can help to identify potential areas of vulnerability or risk. By analyzing the lifeline bars of various objects involved in a transaction or event, fraud detection systems can help to identify patterns and anomalies that may indicate fraudulent activity, and take appropriate action to prevent or mitigate the risk of fraud.

EXPERIMENT – 13

DATE :	5/4/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

Data Flow Diagrams :

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It can be manual, automated, or a combination of both.


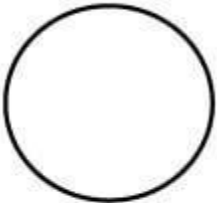

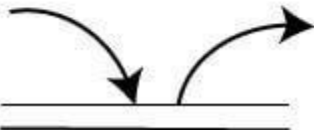
It shows how data enters and leaves the system, what changes the information, and where data is stored.

The objective of a DFD is to show the scope and boundaries of a system as a whole. It may be used as a communication tool between a system analyst and any person who plays a part in the order that acts as a starting point for redesigning a system. The DFD is also called as a data flow graph or bubble chart.

The following observations about DFDs are essential:

1. All names should be unique. This makes it easier to refer to elements in the DFD.
2. Remember that DFD is not a flow chart. Arrows in a flow chart that represents the order of events; arrows in DFD represents flowing data. A DFD does not involve any order of events.
3. Suppress logical decisions. If we ever have the urge to draw a diamond-shaped box in a DFD, suppress that urge! A diamond-shaped box is used in flow charts to represent decision points with multiple exists paths of which the only one is taken. This implies an ordering of events, which makes no sense in a DFD.
4. Do not become bogged down with details. Defer error conditions and error handling until the end of the analysis.

Standard symbols for DFDs are derived from the electric circuit diagram analysis and are shown in fig:

Symbol	Name	Function
	Data flow	Used to Connect Processes to each , other , to sources or Sinks; te arrow head indicates direction of data flow.
	Process	Performs Some transformation of Input data to yield output data.
	Source of Sink (External Entity)	A Source of System inputs or Sink of System outputs.
	Data Store	A repository of data; the arrow heads indicate net inputs and net outputs to store.

Symbols for Data Flow Diagrams

Circle: A circle (bubble) shows a process that transforms data inputs into data outputs.

Data Flow: A curved line shows the flow of data into or out of a process or data store.

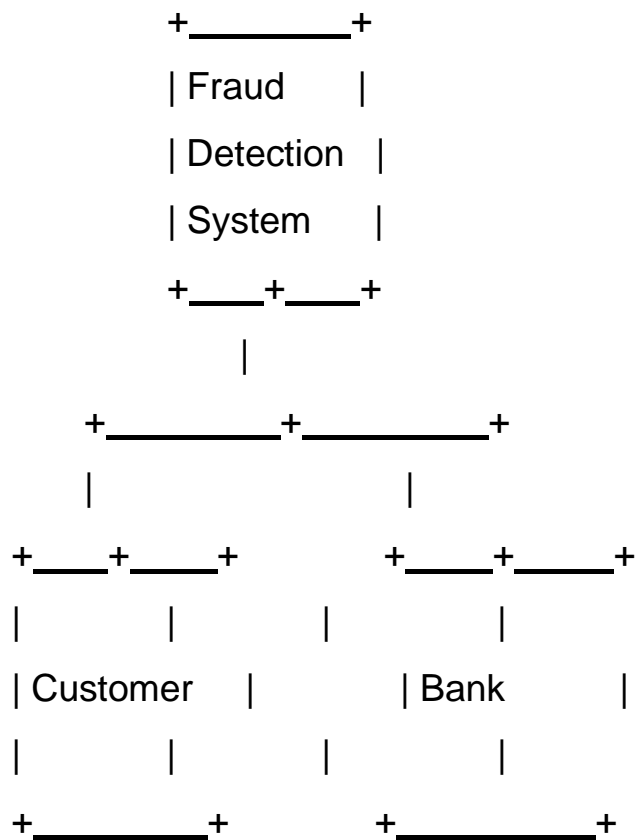
Data Store: A set of parallel lines shows a place for the collection of data items. A data store indicates that the data is stored which can be used at a later stage or by the other processes in a different order. The data store can have an element or group of elements.

Source or Sink: Source or Sink is an external entity and acts as a source of system inputs or sink of system outputs.

CONTEXT DIAGRAM :

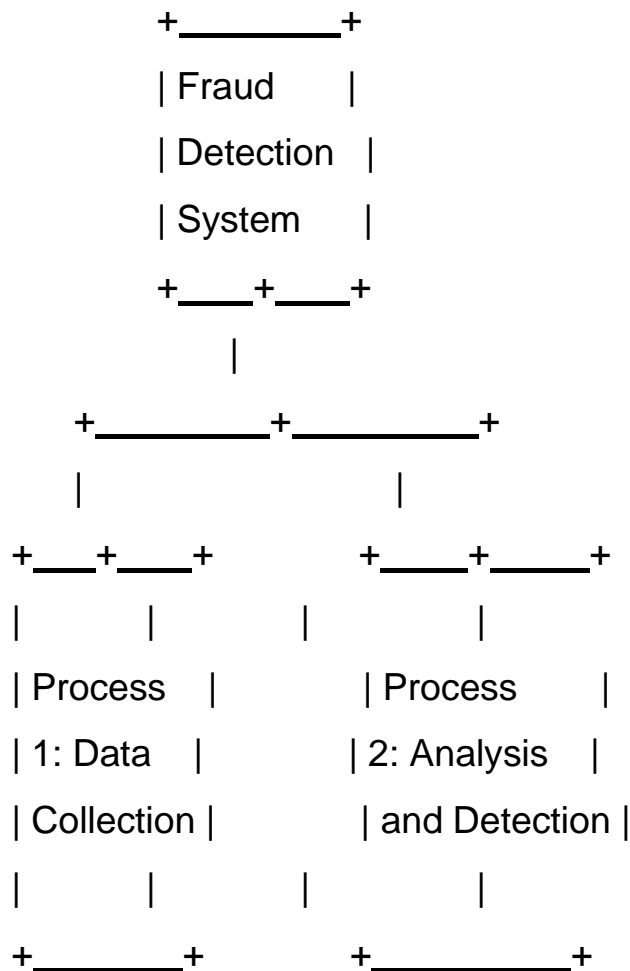
A context diagram for fraud detection system would show the system as a single process or entity, and its interactions with external entities.

Here's an example:



In this diagram, the fraud detection system is shown as a single entity, and its interactions with external entities (customers and banks) are shown with arrows.

Next, we can create a level-0 DFD, which shows the high-level processes that make up the fraud detection system. Here's an example:



LEVELS IN DATA FLOW DIAGRAMS (DFD) :

The DFD may be used to perform a system or software at any level of abstraction. Infact, DFDs may be partitioned into levels that represent increasing information flow and functional detail. Levels in DFD are numbered 0, 1, 2 or beyond. Here, we will see primarily three levels in the data flow diagram, which are: 0-level DFD, 1-level DFD, and 2-level DFD.

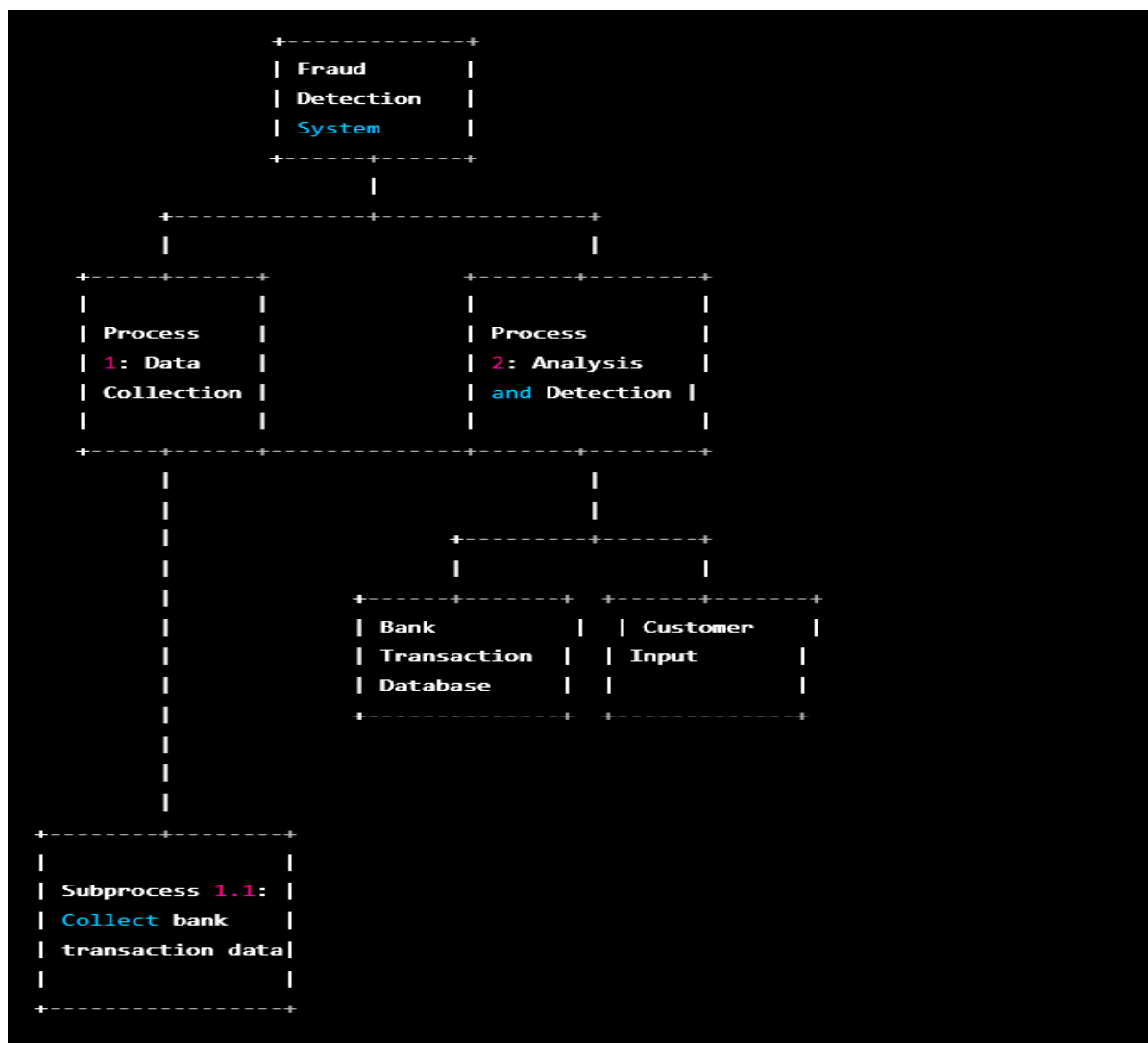
In this level-0 DFD, the fraud detection system is broken down into two high-level processes: data collection and analysis/detection. These processes are shown as bubbles, with arrows indicating the flow of data between them and the external entities.

From here, we could create level-1 DFDs for each of the high-level processes, breaking them down into more detailed subprocesses as

needed. For example, the data collection process might involve subprocesses for collecting transaction data from banks and customer input, while the analysis and detection process might involve subprocesses for pattern recognition and alert generation.

Based on the high-level processes identified in the level-0 DFD (data collection and analysis/detection), we can break each process down into more detailed subprocesses.

Here's an example of a level-1 DFD for the data collection process:



In this level-1 DFD, the data collection process has been broken down into a subprocess (Subprocess 1.1) for collecting bank transaction data. The subprocess interacts with the Bank Transaction Database, which stores transaction data from banks.



In this level-1 DFD, the analysis/detection process has been broken down into two subprocesses (Subprocess 2.1 and Subprocess 2.2). Subprocess 2.1 involves pattern recognition to identify potential fraud, while Subprocess 2.2 generates alerts for further investigation based on the results of Subprocess 2.1.

Leveling a DFD (Data Flow Diagram) is a process of breaking down a complex DFD into smaller, more manageable sub-diagrams. The result is a series of diagrams that show increasingly detailed views of the system being modeled.

TYPES OF DFD:

- The Level 0 DFD shows the high-level view of the online fraud detection system and its interaction with the Online Store.
- The Level 1 DFD breaks down the Fraud Detection Sub-System into its components and shows its interactions with the Online Store and Payment Gateway.
- The Level 2 DFD shows the internal components of the Fraud Detection Sub-System and their interactions. The Data Collection component is responsible for collecting and processing data from the Online Store and Payment Gateway.

EXPERIMENT – 14

DATE :	12/4/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

ADDITIONAL REQUIREMENT:

- ❖ There are several additional requirements for online fraud detection that are essential for ensuring the security of online transactions. Here are some examples:
- ❖ **Real-time monitoring:** Online fraud detection systems must be able to monitor transactions in real-time to quickly identify and respond to fraudulent activities.
- ❖ **Machine learning algorithms:** Fraud detection systems should use machine learning algorithms that can learn and adapt to new fraud patterns.
- ❖ **Multi-factor authentication:** Implementing multi-factor authentication, such as two-factor authentication, can reduce the risk of fraudulent activities.
- ❖ **Device identification:** Fraud detection systems should be able to identify the device used for the transaction and track any changes in device behavior.
- ❖ **Geographic location tracking:** Tracking the geographic location of the user can help detect fraudulent activities from unexpected locations.

- ❖ **Transaction amount tracking:** Monitoring transaction amounts can help detect unusual or suspicious patterns in spending.
- ❖ **User behavior analysis:** Analyzing user behavior, such as browsing history and purchasing patterns, can help identify suspicious activity.
- ❖ Overall, a comprehensive online fraud detection system should incorporate multiple layers of security measures to ensure the safety of online transactions.

ADDITIONAL USES ONLINE FRAUD DETECTION:

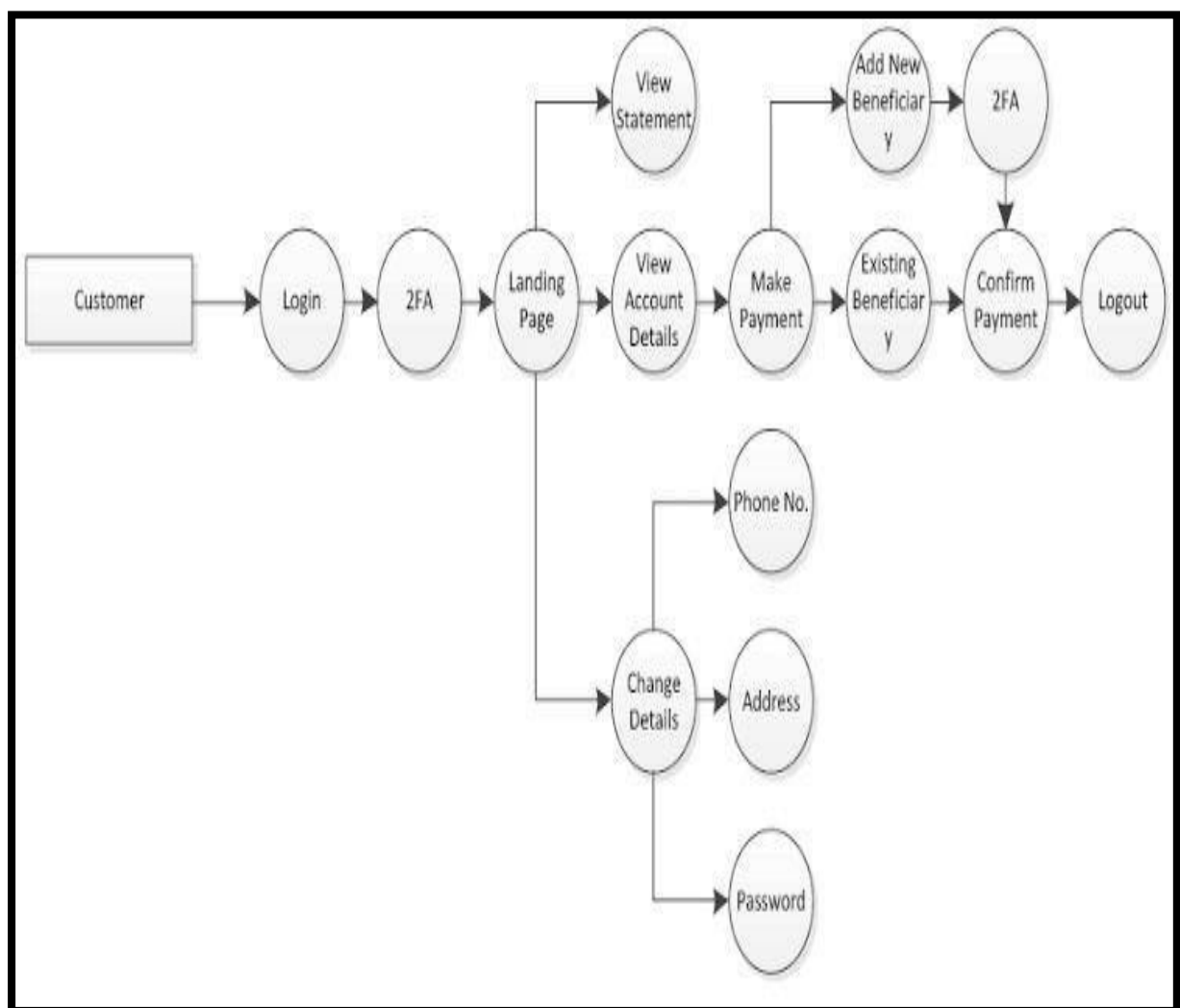
- ❖ Besides detecting and preventing fraud in online transactions, online fraud detection techniques can be applied to other areas as well. Here are some examples:
- ❖ **Identity verification:** Online fraud detection techniques can be used to verify the identity of users during the registration process, preventing the creation of fake accounts.
- ❖ **Insurance fraud:** Insurance companies can use online fraud detection techniques to detect fraudulent claims, such as false accident reports or exaggerated damage claims.
- ❖ **Healthcare fraud:** Healthcare providers can use online fraud detection techniques to detect fraudulent claims, such as overbilling or billing for services not rendered.

- ❖ **Banking and finance:** Online fraud detection techniques can be used by banks and financial institutions to detect and prevent money laundering, fraudulent credit card transactions, and other financial crimes.
- ❖ **E-commerce:** Online retailers can use fraud detection techniques to detect fraudulent purchases and prevent chargebacks.
- ❖ **Online gaming:** Online gaming platforms can use fraud detection techniques to detect cheating, such as the use of bots or other automated systems.
- ❖ **Travel and hospitality:** Online fraud detection techniques can be used to detect fraudulent bookings or reservations, such as fake credit card information or booking multiple rooms using the same credit card.
- ❖ Overall, online fraud detection techniques can be applied to a wide range of industries to improve security, prevent fraud, and protect customers from financial losses.
 - However, it's essential to keep in mind that fraudsters are continually developing new techniques to evade detection. Therefore, businesses need to be proactive in updating and improving their fraud detection systems to stay ahead of the curve. Online fraud detection is an ongoing process that requires constant vigilance and continuous improvement to ensure the security of online transactions.
 - Online fraud detection techniques can be applied to various industries, including banking and finance, e-commerce, insurance, healthcare, travel and hospitality, and online gaming, among others

EXPERIMENT – 15

DATE :	13/4/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

CONTROL FLOW DIAGRAM :



- Here's a general control flow of an online fraud detection system:
- **Data Collection:** The system collects data from various sources such as payment gateways, customer information, and transaction history.
- **Data Preprocessing:** The collected data is preprocessed to remove any irrelevant or redundant information and to convert it into a format that is suitable for analysis.
- **Feature Extraction:** Relevant features are extracted from the preprocessed data, such as the user's IP address, transaction amount, transaction frequency, device information, etc.
- **Model Building:** A machine learning model is built using the extracted features. This model is trained using historical data to detect patterns and anomalies that indicate fraudulent behavior.
- **Real-time Detection:** The system continuously monitors incoming transactions and compares them against the trained model. If a transaction is flagged as potentially fraudulent, it is further investigated.
- **Risk Assessment:** The system assesses the level of risk associated with a flagged transaction based on various factors such as the transaction amount, the user's history, and the type of transaction.
- **Action:** Based on the level of risk associated with the transaction, the system may take appropriate action, such as blocking the transaction, flagging it for manual review, or allowing it to proceed.

Optimum Value of Cyclomatic Complexity :

Cyclomatic complexity of a code section is the quantitative measure of the number of linearly independent paths in it. It is a software metric used to indicate the complexity of a program. It is computed using the Control Flow Graph of the program. The nodes in the graph indicate the smallest group of commands of a program, and a directed edge in it connects the two nodes i.e. if second command might immediately follow the first command.

For example, if source code contains no control flow statement then its cyclomatic complexity will be 1 and source code contains a single path in it. Similarly, if the source code contains one if condition then cyclomatic complexity will be 2 because there will be two paths one for true and the other for false.

Mathematically, for a structured program, the directed graph inside control flow is the edge joining two basic blocks of the program as control may pass from first to second.

So, cyclomatic complexity M would be defined as,

$$M = E - N + 2P$$

where,

E = the number of edges in the control flow graph

N = the number of nodes in the control flow graph

P = the number of connected components

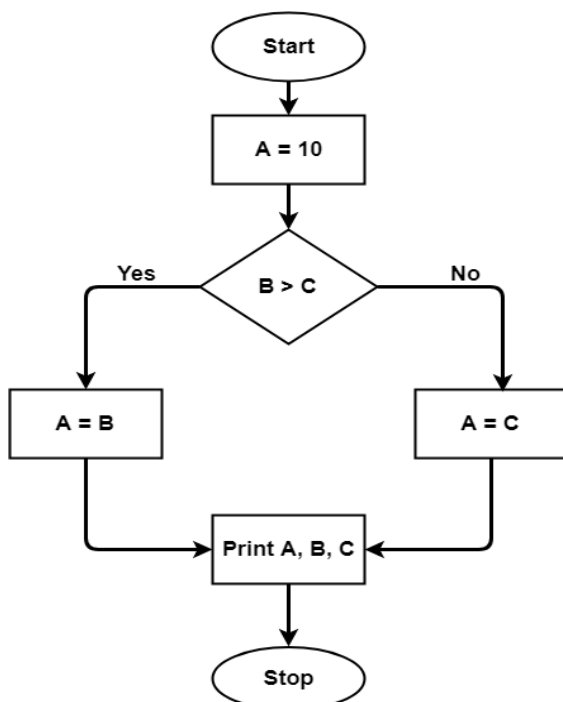
Steps that should be followed in calculating cyclomatic complexity and test cases design are:

- Construction of graph with nodes and edges from code.
- Identification of independent paths.
- Cyclomatic Complexity Calculation
- Design of Test Cases

Let a section of code as such :

```
A = 10
IF B > C THEN
  A = B
ELSE
  A = C
ENDIF
Print A
Print B
Print C
```

Control Flow Graph of above code :



The cyclomatic complexity calculated for above code will be from controlflow graph. The graph shows seven shapes(nodes), seven lines(edges), hence cyclomatic complexity is $7-7+2 = 2$.

Advantages of Cyclomatic Complexity :

- It can be used as a quality metric, gives relative complexity of various designs.
- It is able to compute faster than the Halstead's metrics.
- It is used to measure the minimum effort and best areas of concentration for testing.
- It is able to guide the testing process.
- It is easy to apply.

Disadvantages of Cyclomatic Complexity :

- It is the measure of the program's control complexity and not the data complexity.
- In this, nested conditional structures are harder to understand than non-nested structures.
- In case of simple comparisons and decision structures, it may give a misleading figure.

EXPERIMENT – 16

DATE :	13/4/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

SOFTWARE TESTING:

- Software testing is an essential part of ensuring that an online fraud detection system functions as intended. Here are some aspects of software testing that may be relevant to online fraud detection:
- **Functional Testing:** Functional testing ensures that the system meets the specified requirements and operates as expected. In online fraud detection, functional testing would involve ensuring that the system accurately identifies and flags potential fraudulent transactions.
- **Performance Testing:** Performance testing checks the system's ability to handle a specific amount of workload and its response time. In online fraud detection, performance testing would involve testing the system's ability to handle a high volume of transactions while maintaining accuracy.
- **Security Testing:** Security testing ensures that the system is secure from potential attacks. In online fraud detection, security testing would involve testing the system's ability to protect sensitive data and prevent unauthorized access.
- **Usability Testing:** Usability testing ensures that the system is easy to use and understand. In online fraud detection, usability testing would involve testing the user interface to ensure that it is intuitive and user- friendly.

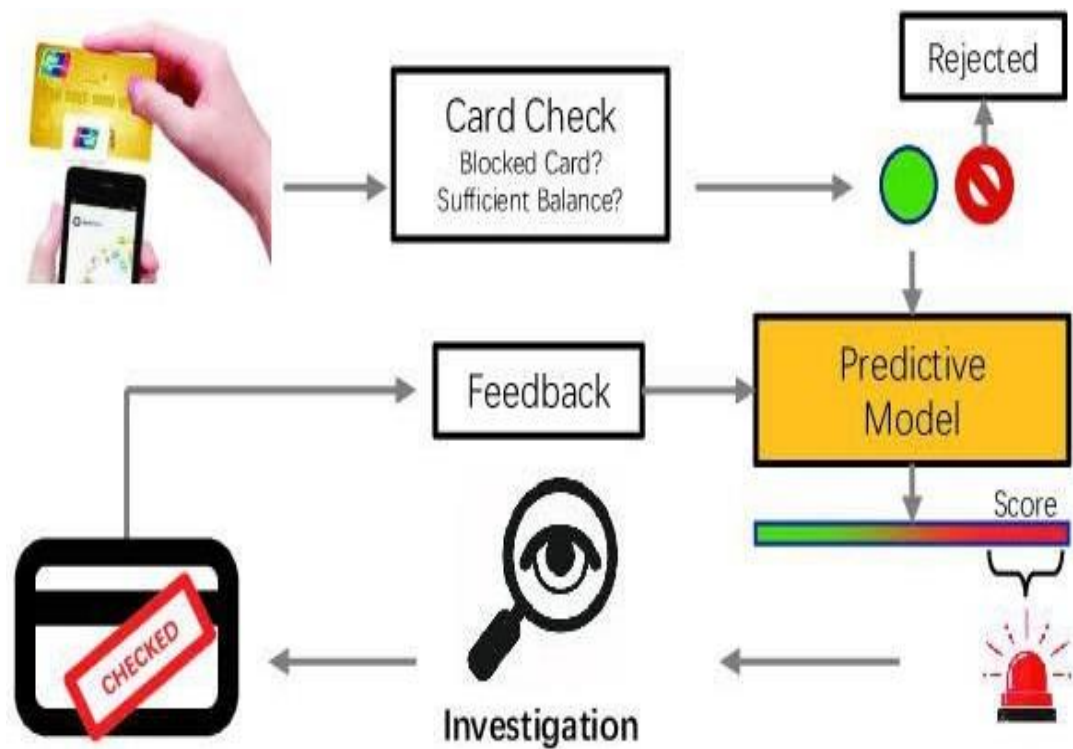
- **Regression Testing:** Regression testing ensures that new changes to the system do not break existing functionality. In online fraud detection, regression testing would involve testing the system after updates or changes to ensure that it still accurately identifies and flags potential fraudulent transactions.
- **Integration Testing:** Integration testing ensures that the different components of the system work together as intended. In online fraud detection, integration testing would involve testing the interaction between different components of the system, such as the fraud detection algorithm and the user interface.



TESTING FRAMEWORKS :

1. There are several testing frameworks that can be used for testing an online fraud detection system. Here are some popular frameworks:
2. **Selenium:** Selenium is an open-source testing framework used for web application testing. It can be used for functional testing of the user interface of the online fraud detection system.
3. **JMeter:** JMeter is an open-source load testing framework used for performance testing. It can be used to simulate a high volume of transactions and test the system's response time.
4. **Appium:** Appium is an open-source mobile testing framework used for testing mobile applications. It can be used to test the mobile version of the online fraud detection system.
5. **OWASP ZAP:** OWASP ZAP is an open-source security testing framework used for web application security testing. It can be used to test the security of the online fraud detection system.
6. **Cucumber:** Cucumber is an open-source testing framework used for behavior-driven development. It can be used to write test cases in a more user-friendly language that can be understood by non-technical stakeholders.
7. **TestNG:** TestNG is an open-source testing framework used for unit and integration testing. It can be used to test the interaction between different components of the online fraud detection system.

8. The choice of testing framework will depend on the specific requirements of the online fraud detection system and the testing needs of the project. It's important to select a framework that can effectively test the critical components of the system and provide reliable and accurate results.



- A testing framework is a set of guidelines, rules, and processes that are used to perform software testing. It provides a systematic approach to testing software and helps to ensure that testing is consistent, repeatable, and efficient.
- A testing framework typically includes tools and libraries that automate testing tasks, define test cases, and manage the test execution process. It also includes a set of best practices for testing, such as test-driven development, continuous integration, and regression testing.

MASTER TEST PLAN :

- A master test plan (MTP) is a high-level document that describes the testing approach and strategies for a project. Here is an example of an MTP for an online fraud detection system:

Introduction:

- The purpose of the MTP is to provide an overview of the testing approach for the online fraud detection system. This document outlines the testing objectives, scope, and strategies to ensure the quality of the system.

Testing Objectives:

- The testing objectives of the online fraud detection system are to ensure that it accurately identifies and flags potential fraudulent transactions, is secure and reliable, and meets the specified requirements.

Scope of Testing:

- The scope of testing includes functional, performance, security, and usability testing. The system will be tested under various conditions to ensure that it meets the expected performance and security standards.

Test Environment:

- The test environment includes the hardware, software, and network configurations required for testing. The environment will be configured to simulate the production environment as closely as possible.

Testing Approach:

- The testing approach includes the testing strategies, methodologies, and tools to be used for testing. The approach will include both manual and automated testing, and the testing strategies will be based on the risk analysis and prioritization of features.

Test Schedule:

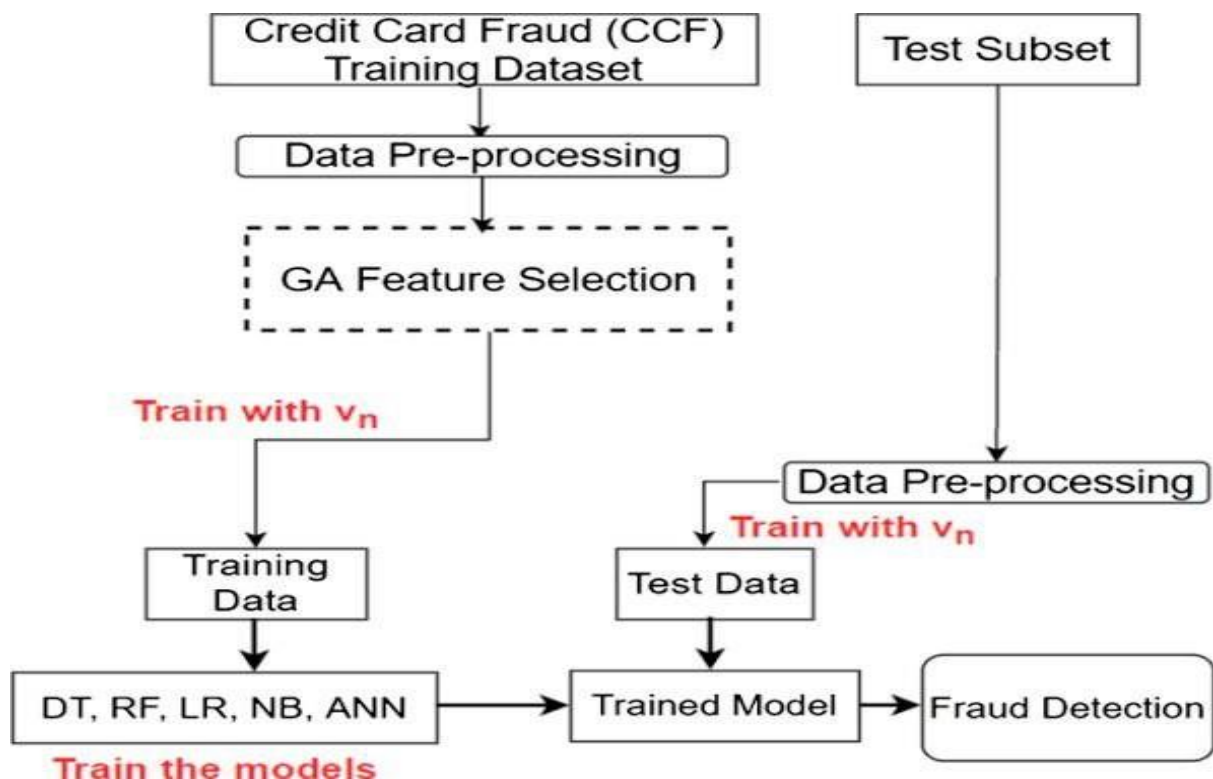
- The test schedule includes the timelines for each testing phase, including planning, preparation, execution, and reporting. The schedule will be adjusted based on the project's progress and the availability of resources.

Risks and Mitigation:

- The risks associated with testing, such as test environment issues, data privacy, and test automation, will be identified and mitigated in the MTP.

Approval:

- The MTP will be reviewed and approved by the project stakeholders, including the development team, testing team, and project manager.



MANUAL TESTING :

- Manual testing can be an essential part of testing an online fraud detection system, especially when testing the user interface and specific functionality that cannot be easily automated. Here are some areas where manual testing can be performed in an online fraud detection system:
- **User Interface Testing:** User interface testing involves testing the system's graphical user interface (GUI) to ensure that it is easy to use and navigate. This type of testing can be performed manually by testers who interact with the system to ensure that it behaves as expected.
- **Functional Testing:** Functional testing involves testing the system's functionality to ensure that it meets the specified requirements. This can be done manually by testers who perform various tests to ensure that the system works as expected under different scenarios.
- **Compatibility Testing:** Compatibility testing involves testing the system's compatibility with various devices, operating systems, and browsers. This type of testing can be performed manually by testers who test the system on different platforms and configurations.
- **Usability Testing:** Usability testing involves testing the system's usability to ensure that it is easy to use and understand. This type of testing can be done manually by testers who interact with the system to identify any usability issues.
- **Security Testing:** Security testing involves testing the system's security features to ensure that it is secure from any external attacks. This type of testing can be done manually by testers who try to identify any security vulnerabilities in the system.

- **Performance Testing:** Performance testing involves testing the system's performance under different load conditions. This type of testing can be done manually by testers who simulate high-volume transactions to ensure that the system's performance does not degrade under heavy loads.
- Manual testing can be time-consuming and may not be able to cover all possible scenarios. However, it is essential for identifying user experience issues and testing edge cases that cannot be easily automated. A combination of manual and automated testing can provide a comprehensive testing strategy for an online fraud detection system.



EXPERIMENT – 17

DATE :	13/4/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

DEPLOYMENT REPORT :

A deployment report for online fraud detection should provide a comprehensive overview of the fraud detection system, including its purpose, design, implementation, testing, and deployment. The report should be written in a clear and concise manner, and should include the following key sections:

1. Introduction: This section should provide an overview of the purpose of the fraud detection system, the problem it is intended to solve, and the scope of the deployment.
2. Design: This section should describe the design of the fraud detection system, including the algorithms, models, and techniques used to detect and prevent fraud. It should also describe the system architecture, data flow, and user interface.
3. Implementation: This section should provide details on how the fraud detection system was implemented, including the programming languages, frameworks, and tools used. It should also describe the database schema and any external APIs or services used.

4. Testing: This section should describe the testing approach used for the fraud detection system, including the types of tests performed, the tools and frameworks used, and the results of the testing. It should also include any issues or bugs identified during testing and how they were addressed.
5. Deployment: This section should describe how the fraud detection system was deployed, including the hardware and software requirements, the deployment process, and any challenges or issues encountered during deployment.
6. Performance: This section should provide an overview of the performance of the fraud detection system, including the accuracy, precision, and recall of the system, as well as any other metrics that are relevant to the system's performance.
7. Conclusion: This section should provide a summary of the key findings and recommendations for future improvements to the fraud detection system.

Overall, the deployment report should provide a detailed and comprehensive overview of the fraud detection system, and should be useful for stakeholders such as developers, project managers, and business analysts who are involved in the deployment and maintenance of the system.

EXPERIMENT – 18

DATE :	13 /4/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

CONCLUSION:

- In conclusion, online fraud detection is a critical aspect of protecting businesses and consumers from fraudulent activities that occur online. With the increasing use of online transactions, it is essential to have robust fraud detection systems that can identify and prevent fraudulent activities in real-time.
- Online fraud detection involves the use of sophisticated software and algorithms that analyze various data points, such as transaction history, user behavior, and other contextual factors, to detect and prevent fraud. However, it is important to note that fraudsters are constantly evolving their tactics and finding new ways to circumvent fraud detection systems.
- To combat this, businesses must continually update and improve their fraud detection systems and processes. This includes regularly testing and evaluating the software to ensure that it is effective in identifying and preventing fraudulent activities.
- Overall, online fraud detection is an ongoing battle between fraudsters and businesses, but with the right technology, processes, and testing in place, it is possible to significantly reduce the risk of online fraud and protect both businesses and consumers.

EXPERIMENT – 19

DATE :	13/4/23
SUBMITTED BY :	N. SAI SADWIK REDDY SHIVNATH CHIRANJEEVI K.VENKATA RAMA SUJAL
TITLE :	<i>ONLINE FRAUD DETECTION</i>

REFERENCES :

1. Google.com
2. Wikipedia.com
3. "A Survey on Fraud Detection Techniques for Online Social Networks" by Ahmed Al-Aamri and Ehab Al-Shaer, IEEE Access, Vol. 5, Pages 21381- 21406.
4. "Combating Online Fraud: A Review" by Adrian Baldwin, Computers & Security, Vol. 72, Pages 223-238
5. "Detecting Fraud in Online Auctions: A Review" by Marco Alberti, Francesco Calabrese, and Fabio Martinelli, ACM Computing Surveys, Vol.51, Issue 3, Pages 1-36
6. "Fraud Detection and Prevention" by IBM:
<https://www.ibm.com/analytics/fraud-detection-and-prevention>
7. "Online Fraud Detection: Techniques and Strategies" by Sift Science:
<https://sift.com/resources/online-fraud-detection-techniques-strategies/>
8. "Online Fraud Detection" by RSA:
<https://www.rsa.com/en-us/solutions/online-fraud-detection>