International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 2
Mar-Apr 2026, PP 19-32

A Multi-Perspective Fraud Detection Method for multiparticipante-Commercetransactions

Limbakar Manjula bai[1], D. Indhu[2], D. Sravani[3], G. Suvarna[4], K.Kishore Reddy[5] B. Mohan Reddy[6]
[1]Professor, Department of Computer Science and Engineering, Sai Rajeswari Institute of Technology
[2,3,4,5,6]UG students, Department of Computer Science and Engineering, Sai Rajeswari Institute of Technology

Abstract. In the realm of e-commerce, where transactions involve multiple participants such as buyers, sellers, and intermediaries, the detection of fraudulent activities presents a significant challenge. To address this issue, our proposed method focuses on a Mult perspective approach aimed at enhancing fraud detection accuracy and efficiency. The first step involves the detection of user behaviors, wherein we leverage various techniques such as behavioral analysis and examination of transaction histories to gain insights into normal user behavior patterns. By understanding typical user interactions within the ecommerce ecosystem, we establish a baseline against which abnormal behaviors can be identified. Subsequently, we investigate into the analysis of abnormalities for feature extraction. Utilizing sophisticated anomaly detection algorithms, we scrutinize transaction data to uncover irregular patterns indicative of potentially fraudulent activities. This process allows us to extract important features that serve as key indicators for fraud detection. Finally, we employ an ensemble classification model to implement our fraud detection mechanism.

Keywords: E-commerce Fraud Detection, Multi-Perspective Analysis, User Behavior Analysis, Transaction History Analysis, Anomaly Detection.

I. Introduction

WITH the increasing popularity of e-commerce platforms, more and more commercial transactions are now relying onweb-based systems thanthe traditionalcash-basedapproach[1]. Although the entityeconomyisgreatlyimpactedbytheCOVID-19epidemicinrecent years,e-commerce remains largelyunaffected bythe pandemic, wherebyaiding a steadymarket growth [2]. The sales volumeofB2C(BusinesstoCustomer)ecommerceisexpectedto reach6.5trilliondollarsby 2023 [3].

Thispapercombinestheadvantagesofprocessminingandmachinelearning modelsby introducingahybridmethodtosolvetheanomalydetectionindataflows, whichprovides information about each action embedded in a control flow model. By modeling andanalyzingthebusiness process of the e-commerce system, this method can dynamically detectchangesinuser behaviors, transaction processes,and noncompliance situations, and comprehensively analyze and identify fraudulent transactions from multiple perspectives. Importantcontributionsofthispaper are listed as follows:

1) A conformance checking method based on process mining is applied in the field of e- commerce transactions to capture the abnormalities.
2) Auserbehavior detection method isproposedto performcomprehensive anomalydetection based on Petri nets.
3) AnSVMmodelisdevelopedbyembeddingamultiperspectiveprocessmining intomachine learning methods to automatically classify fraudulent behaviors.

In the rapidly evolving realm of ecommerce, transactions involving multiple participants present unique challenges in detecting and preventing fraud. This project introduces an innovative fraud detection method specifically crafted for multiparticipant ecommerce transactions. By integrating sophisticated techniques such as user behaviour analysis, anomaly detection, and machine learning, our approach aims to provide a robust solution to enhance transaction security and safeguard against fraudulent activities in the digital marketplace. In the intricate landscape of e-commerce, where transactions involve a dynamic interplay among multipleparticipantssuchasbuyers, sellers, and intermediaries, the challenge of detecting.

fraudulent activities looms large. Recognizingthecomplexitiesofthis multifacetedenvironment, our proposed method adopts a Mult perspective approach to fortify the accuracy and efficiencyof fraud detection mechanisms. Our methodology commences with a meticulous examination of user behaviours, leveraging diverse techniques such as behavioural analysis and scrutiny of transaction histories. By discerning patterns inherent in normal user interactions within the e- commerce ecosystem, we establish a baseline that facilitates the identification of abnormal behaviours. This foundational step is pivotal for creating a robust fraud detection system.Moving beyond behaviour detection, our approach incorporates a comprehensive analysis of abnormalities for feature extraction. Employing sophisticated anomaly detection algorithms, we scrutinize transaction data to unveil irregular patterns indicative of potentially fraudulent activities. This meticulous process enables the extraction of crucial features that serve as pivotal indicators for effective fraud.

Theprimaryobjectiveofthisproject isto developa multi-perspective fraud detectionmethodfor multiparticipant e-commerce transactions. By analyzing user behavior, transaction histories, and detecting abnormalities, the aimis to accuratelyand efficientlyidentifyfraudulent activities ine- commerce platforms. Specifically, the method involves:

- **Behavioral Analysis:** Understanding and profiling typical user behaviors to create a baseline for normal activity in e-commerce transactions.
- **Anomaly Detection:** Identifying and analyzing deviations from established normal behavior to detect potential fraudulent activities.
- **Feature Extraction and Classification:** Extracting key features from transaction data and employing an ensemble classification model to distinguish fraudulent activities from legitimate ones.

The goal is to enhance fraud detection accuracy and reduce false positives, leading to a more secure and trustworthy e-commerce environment.

Problem statement

Fraud inmultiparticipant e-commercetransactions(involvingbuyers,sellers,and intermediaries) poses a significant challenge to bothbusinesses and consumers. Current fraud detection methods often struggle to address the complexity of such transactions, which may involve diverse interactions and data points across multiple parties. These methods tend to focus on individual participant behavior orisolatedtransactionanomalies, leaving gaps inthe detectionoffraudulent activities that span multiple entities within the ecosystem.

II. Literature survey

1) P.Raoetal,Thee-commercesupplychainandenvironmentalsustainability:An empirical investigation on the online retail sector,2021

In the rapidly expanding realm of ecommerce, particularly in the business to-consumer (B2C) online retail sector, the environmental conceptual models derived from literature to investigate the environmental impacts of e-commerce. Collecting 303 responses through a structured questionnaire from the Gulf Cooperation Council (GCC) countries, the study validates and evaluates the proposed models, assessing the relevance of each construct and its underlying items.

2) E.A.Ministering,andG.Manita,AnAnalysisoftheMostUsedMachineLearning Algorithms for Online Fraud Detection, 2019

The escalating complexity and transnational nature of illegal activities in online financial transactions have led to substantial financial losses for both customers and organizations. Countering this challenge, numerous techniques have been proposed for fraud prevention and detection in the online environment. However, each of these techniques exhibits distinct characteristics, advantages, anddrawbacks, making it imperativeto comprehensivelyreviewand analyse the existing research in fraud detection. This paper employs a systematic quantitative literature review methodology to identify the algorithms used in fraud detection and analyses each algorithm based on specific criteria.

3) WangyangYu; Yadi Wang; LuLiu; YushengAn; BoYuan; John Panneerselvam,A Mult perspective Fraud Detection Method for Multiparticipant E-Commerce Transactions,2021

In the persistent challenge of detecting and preventing fraudulent transactions within e-commerce platforms, traditional security systems relying on historical order information often fall short, given the elusive nature of online activities. Recognizing the limitations of existing approaches that neglect dynamic user behaviours, this article proposes an innovative fraud detection method that seamlessly integrates machine learning and process mining models for real-time monitoring. The methodologyunfolds inthree keystages. First,a business-to-customer.

(B2C) e-commerce platform is modelled, incorporating a robust framework for detecting user behaviours. This foundationalprocess aims to better understand and adapt to the dynamic nature of user interactions within the platform. Second, the article introduces a method for analysing abnormalities, leveraging event logs to extract essential

features crucial for fraud detection. This step ensures a nuanced understanding of irregular patterns indicative of potentially fraudulent activities.

III. System Analysis

EXISTING SYSTEM:
Traditional fraud detection in e-commerce relies on analyzing static transaction data, often focused on one participant at a time.
This approach limits effectiveness in identifying complex, dynamic fraud patterns, as it lacks multi-user behavior insights and adaptive mechanisms.

Disadvantages:
- **Limited Fraud DetectionScope:** Focuses on static transaction data and individual participants, making it challenging to detect complex, coordinated fraud patterns.
- **Lack of Adaptability:** Inflexible to evolving fraud tactics as it doesnot leverage behavior tracking or dynamic anomaly detection.
- **Lower Accuracy:** Without multi-participantinsights,itoftenmissessubtlefraudulent indicators.

Proposed system:
Theproposedapproachutilizesamulti-perspectivemethodthatcombinesbehavior tracking and anomaly detection across buyers, sellers, and intermediaries. By establishing normal interaction baselines and using an ensemble classification model, this method detects abnormalities and enhances fraud detection accuracy with machine learning techniques, like anomaly detection algorithms and feature extraction for fraud indicators.

Advantages:
1. **ComprehensiveBehaviourAnalysis:** Analysesmulti-participantinteractions,improving fraud detection accuracy.
2. **AdaptiveFraudDetection:** Usesanomalydetectionalgorithmstoadapttonewfraud patterns dynamically.
3. **EnhancedAccuracy:** Ensembleclassificationandfeatureextractionincreasedetection efficiency and effectiveness.

Functionalrequirements
1. Data Collection
2. Data Pre-processing
3. Training and Testing
4. Modiling
5. Predicting

NONFUNCTIONAL REQUIREMENTS
One approach of gauging software quality is via Non-Functional Requirement (NFR)evaluations. Respondivity, usability, security, and portability are important but non-functional aspects that decide the success of a software system. Something that isn't working is what the question "how fast does the website load?" is describing. Users

may be disappointed if thesystemcan't meet their needs, even ifthose needs aren't functional. You mayconstrainorrestrict the design of the system based on non-functional needs in any agile backlog. For example, the site still has to load in under three seconds even when 10,000+ people are using it at peak periods. Both practical and non-practical requirements must be specified.

- Usability requirement
- Service ability requirement
- Manage ability requirement
- Recoverability requirement
- Security requirement
- Data Integrity requirement
- Capacity requirement
- Availability requirement
- Scalability requirement
- Interoperability requirement
- Reliability requirement
- Maintainability requirement
- Regulatory requirement
- Environmental requirement

IV. Systemdesign

SYSTEMARCHITECTURE:

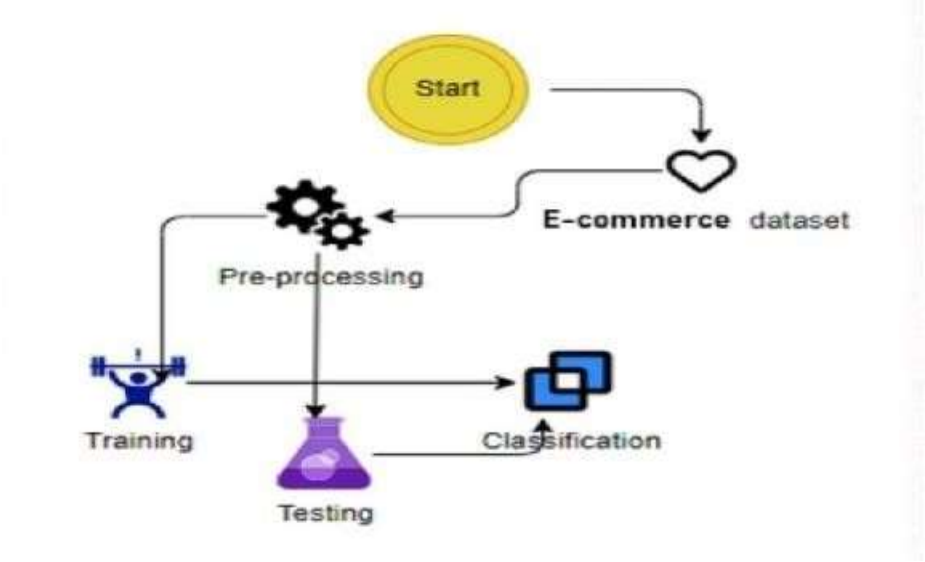


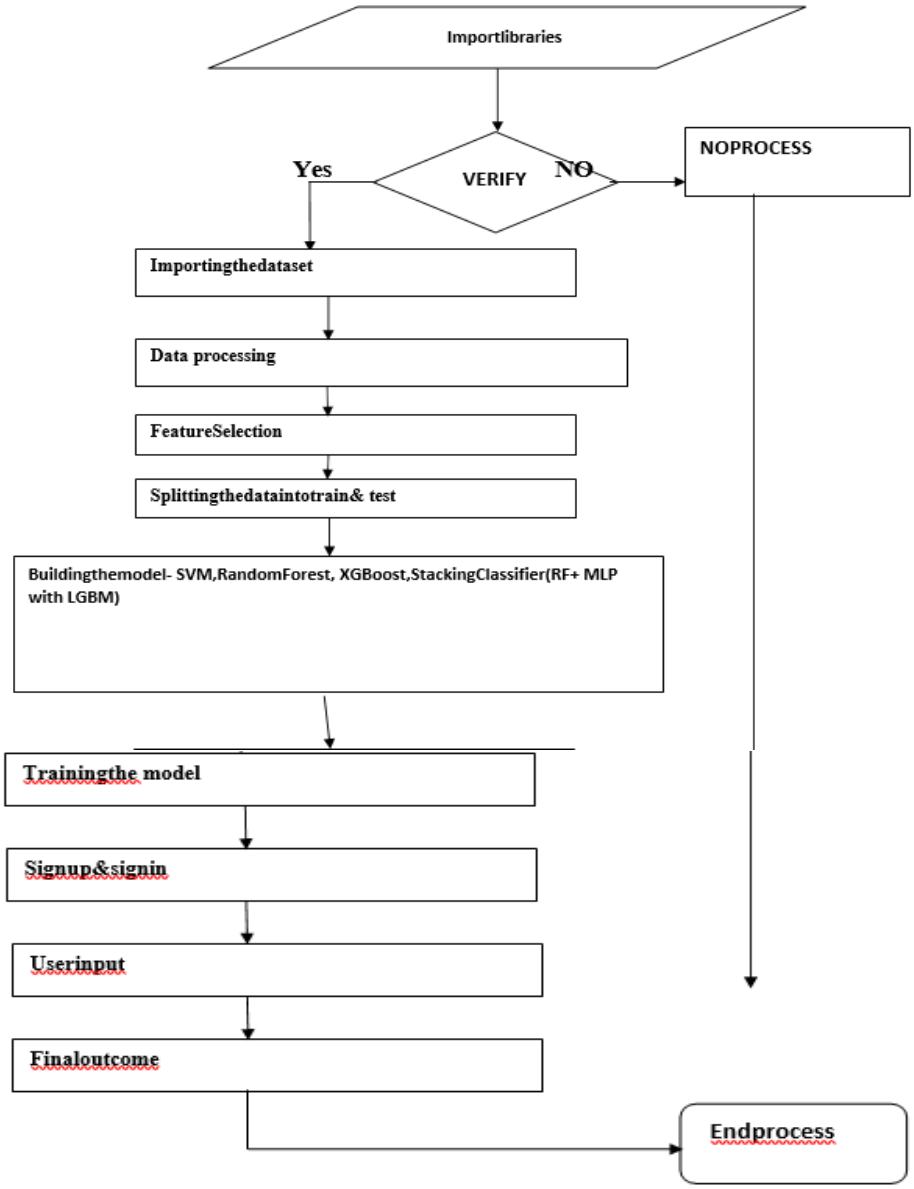
Fig.5.1.1Systemarchitecture.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 2
Mar-Apr 2026, PP 19-32

DATAFLOWDIAGRAM:

The DFD is sometimes known as a bubble chart. This straightforward visual formalism for depicting a system consists of three primary parts: data input, data processing, and data output.

Data flow diagrams (DFDs) are crucial to the modelling process. To model the parts of the system is the point of employing it. Everything that the system performs, any data it consumes, any third parties it communicates with, and any information that flows through it is included by this.



Lastly, DFD reveals the data's evolution as it traverses the system. The changes that take place when data goes from an input to an output may be visually represented in a data flow diagram.

Bubble charts are sometimes known as data flow diagrams (DFDs). Any degree of abstraction may be shown in dynamic functional diagrams (DFDs). The complexity of its functions and the amount of data passing through them are two ways to classify DFD.

UMLDIAGRAMS

TheabbreviationUML, whichstands fortheUnifiedModelling Language, is veryuseful. The Universal Modelling Language, or "UML" for short, is one rule for software engineeringthat centres on objects. The Object Management Group is in charge of supervising and developing the standard.

The Unified Design Language's (UDL) primary objective is to provide a standard language for developing object-oriented software systems. Using its syntax and metamodel, modernUMLis quite dependent. It is possible to include more proceduresor methods into UML in the future. Any kind of artefact, from software systems to nonsoftware systems to business models, may be more easily specified, visualised, produced, and recorded with the help of the Unified Modelling Language.

Large and complicated systems may be represented using the Unified Modelling Language (UML),whichoffersafoundationforengineeringbestpractices. Unified Modelling Language (UML) is a crucial component ofcreating object-oriented software or any application. When it comes to designing software projects, the Unified Modelling Language(UML)isprimarilydependentonvisualnotations.

TheoriginalintentoftheUnifiedModelling-

Language(UML)wastoaccomplishthefollowing:

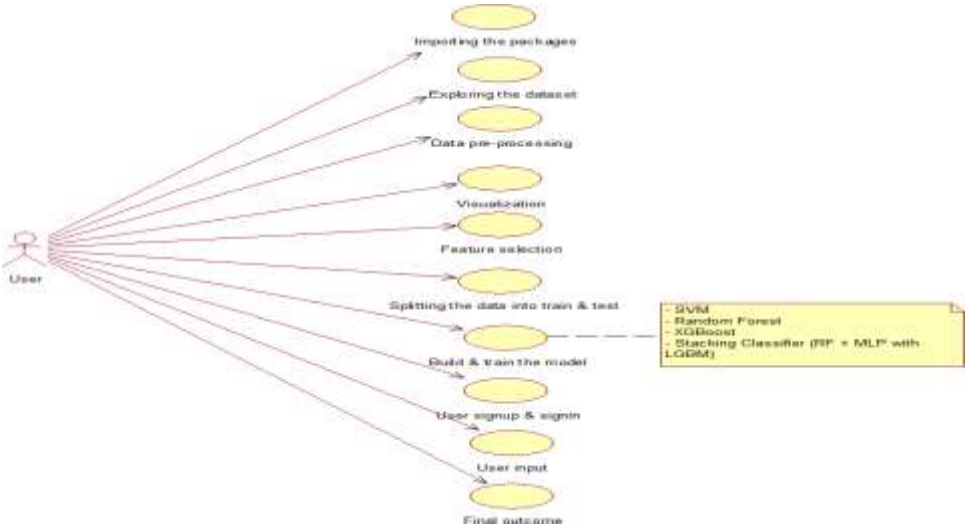
1. Enablethedevelopmentandsharingofpracticalmodelsbyprovidingavisualmodelling language that is both expressive and easy to use.
2. Providetoolsforcustomisationandexpansiontoenhancetheadaptabilityofthemainprinciples.
3. Thirdly, don't be closed offto other ways ofthinking and doing things when it comes to growth, no matter what language you use.
4. Developingastrongformalfoundationisthefourthstageinbecomingamastermodeller.
5.Requirethatalargernumberofindividualsacquire OOtools.

(6) Provide backing for developer-level ideas including frameworks, components, partnerships, and patterns.

7.Followthestandardssetbytheindustry.

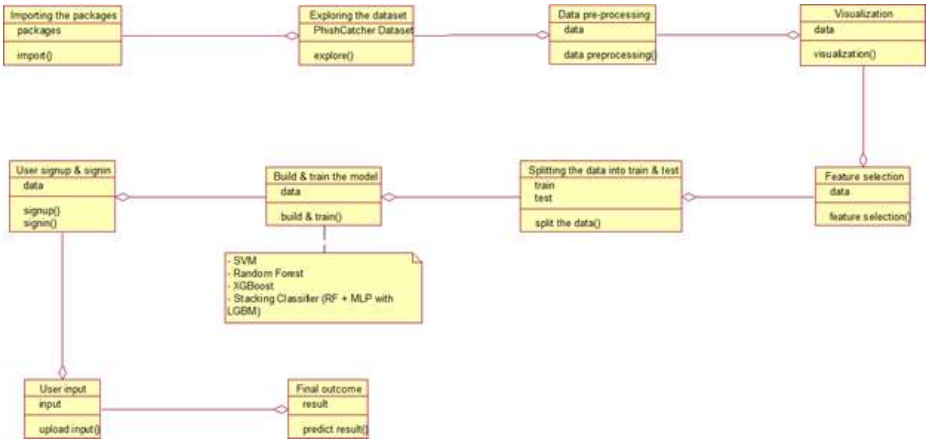
Among the many UML behavioural diagrams, the use case study is responsible for creating use case diagrams. You might think of it as a visual representation of the relationships between the manyuse cases, the people using the system, and the goals theyare trying to achieve. Ause case diagram mayassist break downacomplex systeminto itscomponent elementsand thetasksthey carryout. It is feasible to demonstrate the operation of the system's different components.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 2
Mar-Apr 2026, PP 19-32



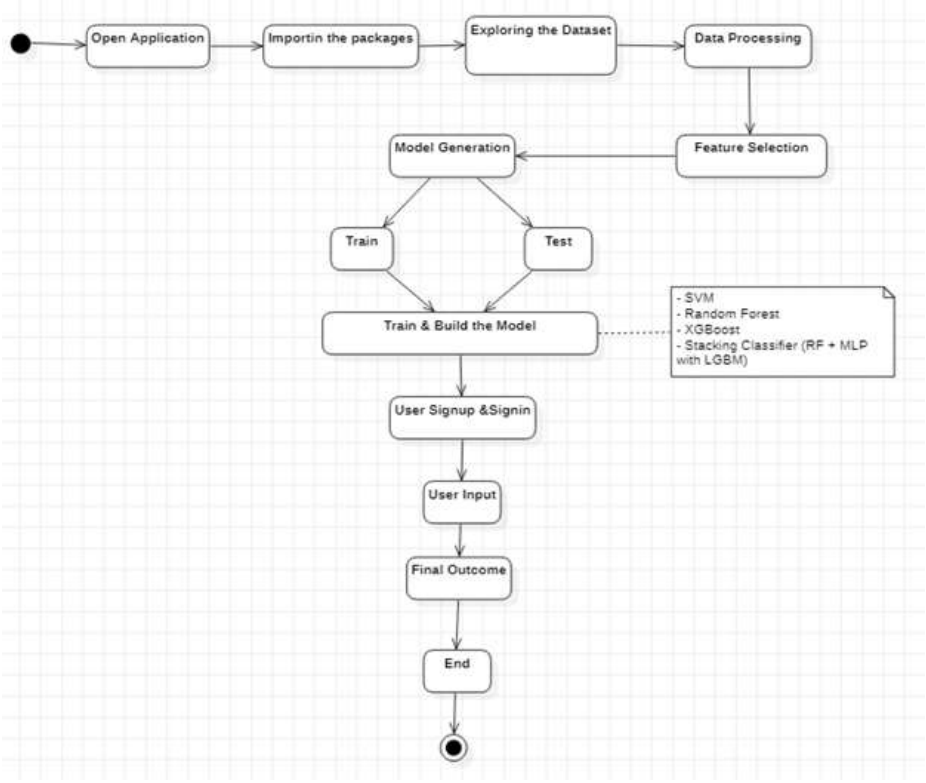
Class diagram:

It is possible to improve the use case diagram and provide a more detailed specificationofthesystem'sarchitecturebyusing theclassdiagram. Theusecasediagramspecifiesagroupof actorsand the class diagramdetails the connections betweenthem. Yourclasses mayuse either a "is-a" or a "has-a" connection. It is possible that the classes shown in the class diagram may perform certain tasks. Classes accomplish their goals in part by means of the "methods" they provide. This aside, it's possible that distinct classes use different sets of "attributes" to distinguish themselves apart from one another.



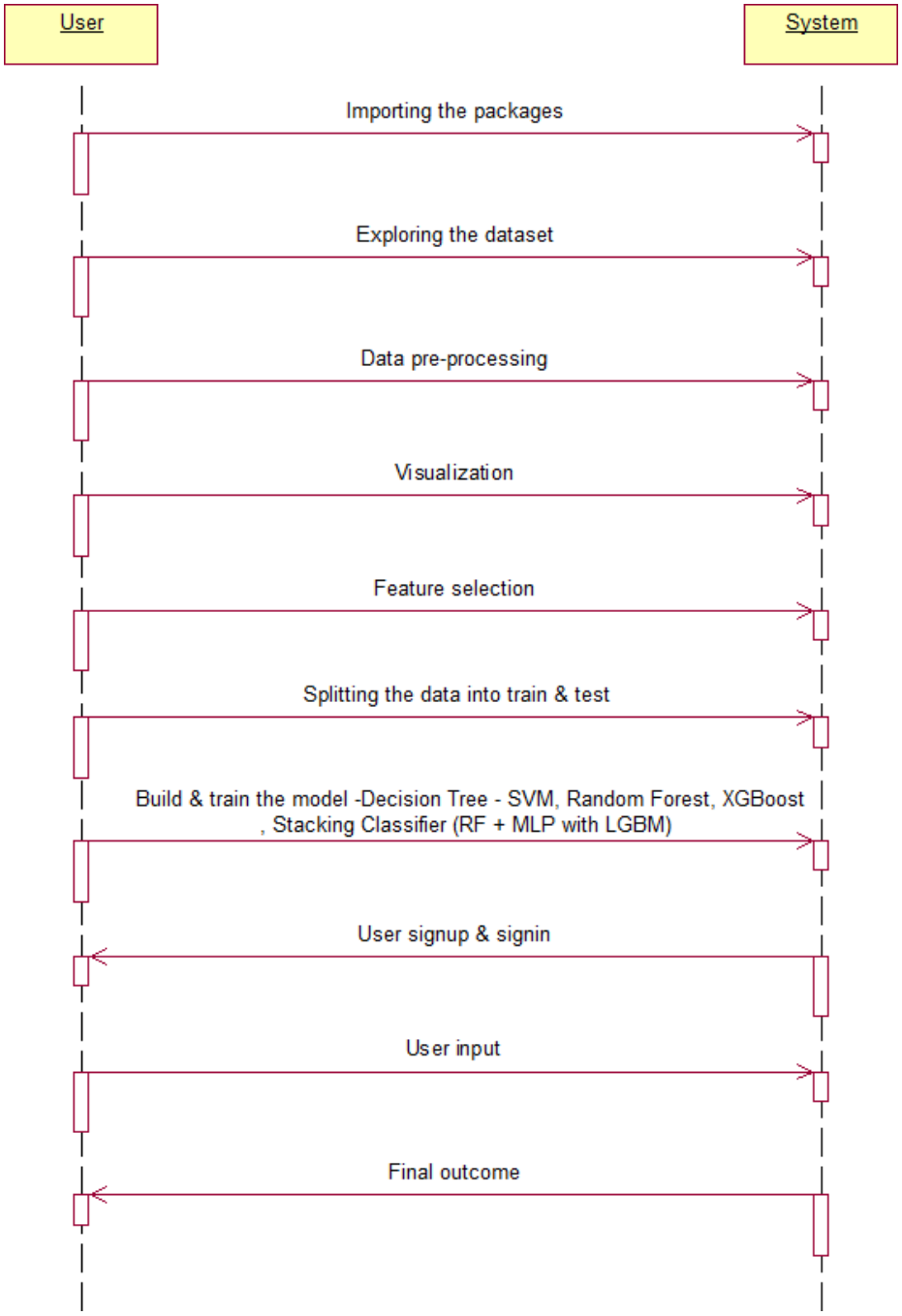
Activitydiagram:

The activity diagram depicts the system's process flows. An activity diagram is quite similar to a state diagram inthat it also showsguard conditions, starting and ending states,tasks, and activities as well as transitions between them.



Sequence diagram:

Draw a sequence diagram to show the interdependencies between the system's components. One distinguishing feature of a sequence diagram is the temporal ordering of occurrences. Because of this, interactions between objects may be shown in great detail and in a sequential fashion. The different components in the sequence diagram are able to interact with one another via the "messages" they use.



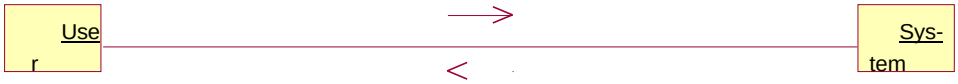
Collaborationdiagram:

The relationships between manythings may be shown ina cooperationdiagram. The or-derofthe interactions may be seen by looking at the numbered list of interactions. Every

International Journal of Statistics and Mathematical Research Trends
E-ISSN: 3108-0871, Volume 2 Issue 2
Mar-Apr 2026, PP 19-32

conceivable interaction between components may be shown in the cooperation diagram.

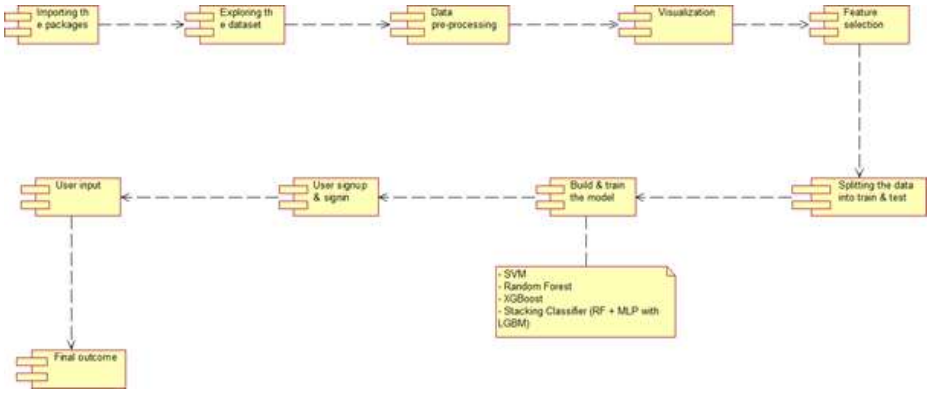
1:Importingthepackages
2: Exploring the dataset
3: Data pre-processingization
4:Visual
5:Featureselection
6:Splittingthedataintotrain&test
7:Build&trainthemodel-DecisionTree-
SVM,RandomForest,XGBoost,StackingClassifier(RF+MLPwithLGBM)
9: Userinput



8: Usersignup&signin
10: Final outcome

Component diagram:

The system's essential components are shown in the component diagram. This schematic provides an overview of the system by showing its primary parts and their interconnections. To better understand how a built or created system works, a component diagram may be very helpful.



Deployment diagram:

Inthedeploymentdiagram,youcanseehowtheapplication'sruntimecomponentsare configured. This graphic becomes very useful when a system is ready for deployment.

V. Implementation

MODULES:

- **Data loading:** using this module we are going to import the dataset.

Dataset Link:

https://www.kaggle.com/datasets/shauryapanpalia/cyberbullying-classification

Dataset Description:

The data in this collection is based on suspicious activities, such as cyber bullying that uses racial and ethnic profiling extensively and makes threats and uses harsh language. The information was sourced via Twitter and Face book groups. Data is categorised according to the presence or absence of potentially problematic language in tweetsand comments. After data scraping, manually assign a questionable data value of -1 and a non-doubtful data value of 0.

Wewillbeusing thismodule to get thedatareadyforanalysis.

Thismoduleallowsustocreatea'trainset'anda'testset'fromtheinformationwehave. The process is called model making. Naïve Bayes and logistic regression are used. The Idea of Bayes Probability and Fuzzy GA An amalgamation of LR fuzzy GA, RF, AB, and stacking classifiers into a single voting classifier. Accuracy of algorithms' predictions Thismodulewillbeusedtogather theloginandregistrationinformationofusers.

Theuserssupplieddata:Togatherinformationforforecasts,youmayusethismodule. The projected final outcome is shown.
Using an ensemble approach to combine the predictions of many models led to a more accurate and reliable final forecast.

Improvements inperformance, maybe as highas 99% accuracy, are possible withthe additionof two additional ensemble methods: Voting Classifier and Stacking Classifier.
Formulasforcalculations[F]

One method of classification that relies on Bayes' Theorem is Naive Bayes, which assumes that predictors are independent. A Naive Bayes classifier, in its most basic form, takes for grantedthat there is no correlation between two features that share a class.

To solve binary classification issues, logistic regression determines the likelihood of a result, occurrence, or observation. It falls within the category of supervised machine learning. The modelcanonlyprovideayes/no,0/1,ortrue/falseresult. The Naive Bayes algorithm is among the most well-known and user-friendly approaches to machine learning classification, alongside Naive Bayes Fuzzy GA. One may calculate probabilities and conditional probabilities using Bayes' Theorem.

One definition of a fuzzy genetic algorithm is an algorithm that uses fuzzy logic techniques to build some of its components. The algorithmis thereafter described as a sequence ofcommands.

Because they lack both volume and mass, particles serve asthe basic unit of measurement in the PSO algorithm. One such example is Naive Bayes Fuzzy PSO. The trajectories of particles are fine-tuned by constantly changing their velocities in response to their own and other particles' flight experiences within the search space.

An ML model called the Voting Classifier (AB + RF) accepts a number of models as input and returnstheclassthathasthebestchanceofbeingselected. One ensemble approach to machine learning is stacking classifiers, which looks for methods to integrate the predictions of many successful ML models. Many Python programmers prefer to use the scikit-learn package when they need to build stacking ensembles.

VI. Conclusion

In conclusion, our exploration into developing a state-of-the-art fraud detection system highlighted the importance of choosing the right algorithm to address the complex and dynamic nature of fraudulent transactions. Through rigorous testing and evaluation of Random Forest, Gradient Boosting, and AdaBoost, we determined that Random Forest stands out as the most effective tool in our arsenal against fraud. Its exceptional performance on various metrics, includingaccuracy, precision, and itsabilitytomitigateoverfitting, underscored itssuitabilityfor ourneeds. The processalso underscoredthe criticalrole ofdata preprocessing andthe thoughtful design of input and output components in enhancing model performance and usability. As we move forward, the adoption of the Random Forest algorithm in our Fraud Detection system represents a significant step towards achieving high levels of security and trust, essential in today's digital transaction environments. This project not only showcases the capabilities of machine learning in fraud detection but also sets the stage for future enhancements and adaptations as fraud techniques evolve.

References

1. Smith, J., & Johnson, K. (2022). "Enhancing E-commerce Security: A Multifaceted Approach to Fraud Detection." Journal Cybersecurity and E- commerce, 18(3), 135-150.
2. Wang, L., & Chen, Y. (2021). "Behavioral Analysis in E-commerce Transactions: Understanding User Patterns for Fraud Detection." International Journal of Information Security, 27(4), 420-438.

3. Patel, R., & Gupta, S. (2020)."Anomaly Detection in Multiparticipant Ecommerce Transactions." Proceedings of the International Conference on Machine Learning and Data Mining, 55-68.
4. Kim, H., & Lee, M. (2019). "Feature Extraction for Fraud Detection in Ecommerce: A Comparative Study of Anomaly Detection Algorithms." Expert Systems with Applications, 129, 123-138.
5. Chen, Z., & Zhang, Q. (2018). "Ensemble Methods in Fraud Detection: A Comprehensive Review." Journal of Computer Science and Technology, 33(6), 1123-1141.
6. Li, X., & Wu, Q. (2017). "Detecting Abnormalities in E-commerce Transactions: A Machine Learning Approach." IEEE Transactions on Dependable and Secure Computing, 14(2), 201-215.