# AI-Powered Insurance Claim Fraud Detection Automobiles (Car) Accidents

Kalyani Priyanka[1], Medishetty Satvika[2], Ravula Soumya[3], Thoutam Khushi[4]
[1,2,3,4]*Department of Computer Science Engineering, Stanley College of Engineering and Technology for Women, Hyderabad, India*

***Abstract*— Insurance fraud results in a huge financial loss for insurance companies every year, which creates a need for developing an efficient system using advanced technologies to identify insurance fraud effectively. This leads to a huge financial loss for insurance firms. The system works by assessing insurance claims based on various parameters such as age of claimants, amount of claim, and time of incident to calculate a score that is required to assess the level of fraud. Random Forest models are efficient in detecting fraudulent insurance claims using supervised learning algorithms with high accuracy. The insurance fraud detection system is developed using React.js to create a dynamic user interface, Node.js/Flask to create efficient backends, and MySQL to manage data efficiently in a full-stack architecture. The experimental results show that using ML models, accuracy in insurance fraud detection is increased and automated decisions in claim processing are enhanced.**

***Index Terms*— Standard in the field include insurance fraud detection, ML models, Random Forest, supervised classification, and claim risk evaluation methodologies.**

## I. INTRODUCTION

Fraudulent insurance claims have been identified as one of the challenges faced by insurance service providers around the globe. Too many fraudulent insurance claims is a big problem that has been affecting insurance firms and has made it difficult for them to carry on their activities. The main fraudulent claims include overstating claims of damage, giving false information during registration, and making claims of things that did not happen. Schemes are changing rapidly and it is becoming difficult to know what is going on since there is a lack of information. It is becoming difficult to identify fraudulent claims and prevent them before incurring losses. With the increasing fraudulent claims in today's growing schemes, it is not possible to investigate claims after they are made or to follow a process that is becoming chronic.

## II. LITERATURE REVIEW

Insurance fraud causes significant financial losses every year. Reports estimate that fraudulent insurance activities result in losses exceeding $300 billion annually, which ultimately increases insurance premiums for customers. The increase in growth during the forecast period can be related to investments in AI-based fraud detection systems, an increase in demand for real-time fraud analytics services, and an increase in cloud-based fraud systems. These systems use historical data and feature engineering to identify abnormal claim behavior and suspicious transactions, ensuring accurate classification of claims.

Surge in Insurance Fraud Driving Growth of the Insurance Fraud Detection Market with rising demand for real-time fraud analytics and expansion of cloud-based fraud platforms. Increasing investments in ai-powered fraud detection and growing focus on cross-channel fraud prevention, with 21% of insurance companies planning to invest in AI in the next two years. These systems rely on historical datasets and feature engineering to identify abnormal claim behavior and suspicious transactions, analyzing data to uncover scams. Hybrid models that combine multiple algorithms and ensemble techniques for fraud detection are being explored with increasing investments in ai-powered fraud detection. Adoption of data-driven fraud prevention tools and rising demand for real-time fraud analytics enable insurance companies to process claims automatically with high detection accuracy.

The proposed system, by using the interpretability of statistical techniques together with the flexibility of

AI, provides a balanced solution that improves both interpretability and efficiency of fraud detection systems.

Machine learning is a pragmatic breakthrough in prediction and finding complex structures and patterns within large data sets, and ensemble methods combine statistical and AI approaches to enhance prediction and stability.

## III. METHODOLOGY

Modules:

- Import the required Python libraries.
- Explore the insurance claims dataset.
- Process and clean the data with the use of the Pandas library.
- Visualize the data with the use of Matplotlib and Seaborn.
- Select features that are important for model.
- Predict the fraud with the use of the trained model.
- Show the results with the use of the GuardRail AI frontend.

A) System Architecture

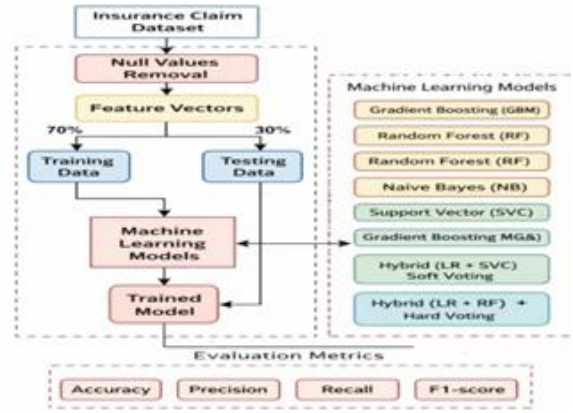



Fig 1. System Architecture

Proposed Work:

By training a ML model on historical claims that were classified as fraudulent or genuine, it is able to learn from this data and subsequently be able to identify potential frauds. Machine learning is able to learn from historical records of claims to identify what makes a claim genuine or not.Some common features used in insurance fraud detection models to analyze the variables include claimant age, claim amount, date and time of incident as well as vehicle information (make, model etc.)Supervised learning has been extensively used to train models based on Random Forest Classifier algorithms using previous insurance claims data, which has established itself as a common approach for predicting fraud. The model generates a fraud probability score for each new claim based on learned patterns from training data to quantify the fraud risk. The table thus presents the claims as accepted or rejected by using a threshold to the fraud probability score of the model and assigned those claims into accepted legitimate or rejected fraudulent.

B) Dataset Collection:

The adoption of model-based interpretability which delivers acceptable predictive performance with relevant results provides a better solution for fraud detection than using post-hoc explanations to analyze more advanced models. The top features in fraud detection differ between segments which creates a solution that improves both interpretability and operational productivity. The machine learning algorithms which data scientists use for their work can enhance their prediction accuracy while enabling researchers to track how model results change with different feature adjustments and discover new knowledge from intricate data sets. The range of interpretability techniques includes basic rule-based models which provide specific decision rules and advanced feature-importance assessments, and ensemble methods that merge statistical and AI models utilize error ratio metrics to create standardized performance evaluation across different challenges.The system works well with good stability using ensemble methods that integrate statistical models and AI models to generate accurate predictions using Shapley Values. Interpretable models allow users to understand their working mechanisms without needing further explanations, and statistical tests and analysis methods like regression analysis and correlation analysis act as global interpretability tools.

| Index | months as customer | age | policy state | policy deductible | incident type | incident severity | vehicles involved | total_claim amount | fraud_reported |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 328 | 48 | OH | 1000 | Single Vehicle Collision | Major Damage | 1 | 71610 | Y |
| 1 | 228 | 42 | IN | 2000 | Vehicle Theft | Minor Damage | 1 | 5070 | N |
| 2 | 134 | 29 | OH | 2000 | Multi Vehicle Collision | Total Loss | 3 | 34650 | N |
| 3 | 256 | 41 | IL | 1000 | Single Vehicle Collision | Major Damage | 1 | 63400 | Y |
| 4 | 228 | 44 | IN | 500 | Vehicle Theft | Minor Damage | 1 | 6500 | N |

C)Pre Processing:

The data cleaning process involves using Pandas in cleaning and organizing untidy data since it provides various tools and functions that can be used in cleaning

data. This involves using `dropna` to remove all rows in the data that have empty values, and data type conversion, which is helpful in preparing data for training an ML model. The use of Seaborn and Matplotlib libraries aids in creating visual representations of data trends. The visualizations show how data patterns connect and how the data distribution works, which helps researchers study insurance claim data. The conversion of categorical attributes into numerical form occurs through label encoding, which allows analysts to process the data. Most machine learning models require numerical data because they use it to learn from data patterns and make predictions.

D)Training & Testing

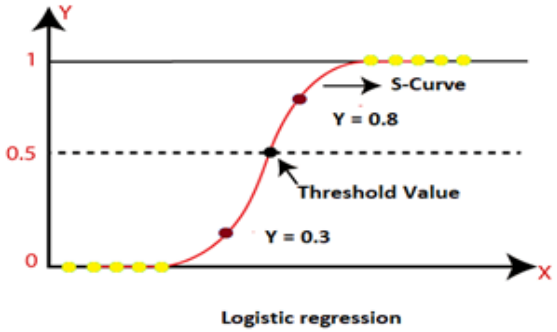
Technical teams should also implement systematic processes for collecting, cleaning, and structuring data that can capture the full complexity of real-world business scenarios; this directly impacts the performance of the model. This is achieved by exposing the model to historical data and allowing it to learn from it, such as learning patterns, relationships, and dependencies within the data set, thereby training and validating the model on the training and validation data set. Testing multiple model architectures is also essential and helps achieve better results for all critical metrics, achieving 20-35% better performance than using a single approach by default, and fine-tuning hyperparameters. After testing and evaluating the model, it is time to deploy the model for production using model deployment and maintenance.

Deployment: Finally, the model has to be deployed in production, even though the diagram shows the last phase, Model Deployment. After the model has been trained on the prepared data, the system tests its performance and evaluates the model with the use of certain metrics in the Model evaluation and testing phase. Organizations experience improved model accuracy rates of 15-30%, and the success metrics include the business, machine learning models (Accuracy, F1 score, AUC), thereby making the model reliable.

Algorithms:

1.Logistic Regression

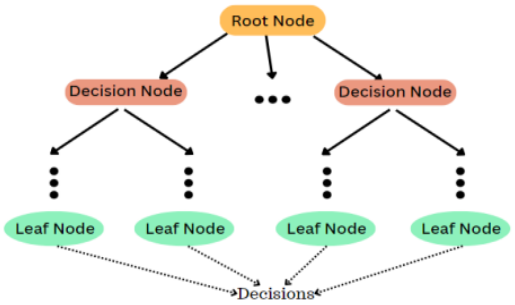
Logistic Regression is a classification-based ML algorithm that utilizes a sigmoid function to analyze a given linear equation to reach a conclusion about whether a given entity belongs to a certain class or not. The logistic regression algorithm is a machine learning algorithm that utilizes a sigmoid function to map a given linear equation to a range between 0 and 1 to reach a conclusion about whether a given entity belongs to a certain class or not. The logistic regression algorithm utilizes a class label generated through a threshold value set to 0.5 by default, where all instances are classified to Class 1 if they are above the threshold and to Class 0 if they are below the threshold. The Gradient Descent algorithm is an optimization algorithm used to reach optimal values by minimizing the Cost Function and maximizing log likelihood.



Logistic regression

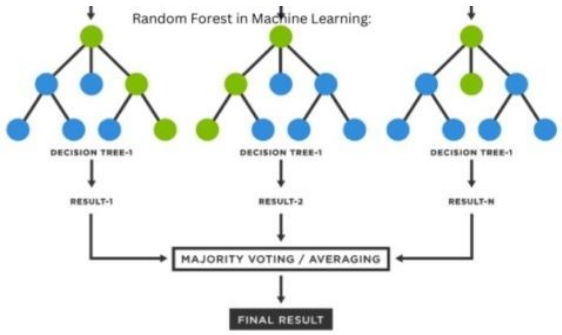
2.Decision Trees

Decision tree is a supervised learning algorithm that is based on a concept called supervised learning, where the given dataset is recursively divided into smaller regions based on the most important features of the given data set. Decision tree is a tree data structure that consists of nodes and branches, where each node represents a feature, each branch represents a value or an outcome of a feature, and each leaf node represents a class label. Decision tree is very useful as it can be understood by a non-technical person, and it is very useful for handling numerical as well as categorical values.



3.Random Forest

Random Forest is an algorithm used by machine learning that brings together many different decision trees to form one and only one result or output.This is achieved through an ensemble of multiple decision trees that are made as diverse as possible through an approach referred to as bootstrap sampling. This is what makes Random Forest so effective in eliminating the high variance that decision trees are so prone to, thus making it more accurate due to diversity.




## IV. EXPERIMENTAL RESULTS

A) Comparison Graphs: Accuracy, Precision, Recall,fl score

Accuracy: Accuracy is a term that is used to define a fraction of all correct predictions made by a model over all claims made by it.

Accuracy is a ratio of all classifications that were correct, whether they were positive or negative, and it gives us an idea of how accurate a model is with its predictions. Accuracy is defined as a ratio of all correct predictions made by a model over the total instances in a dataset.

This might be expressed as:

$$\text{Accuracy} = \frac{(TP + TN)}{(TP + FP + TN + FN)}$$

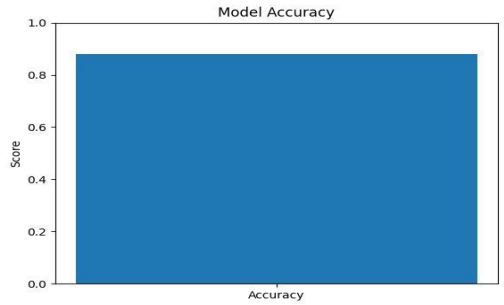



Fig 2: Accuracy Graph

Precision: Precision refers to the total claims made by the model, which are identified as fraudulent compared to the actual fraudulent claims made. A higher value of precision indicates that the system has fewer false alarms for fraud claims.

$$Precision = \frac{TP}{TP + FP}$$

Recall: Recall is used to refer to the ability of the model to identify all the fraudulent claims made in the data set. Recall shows how well the system is able to identify actual fraud claims made in the data set.

$$Recall = \frac{TP}{TP + FN}$$

F1-Score: F1-Score is a good score for balancing the effectiveness of the model. This score can be used for data sets where there are fewer fraudulent claims compared to genuine claims.

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

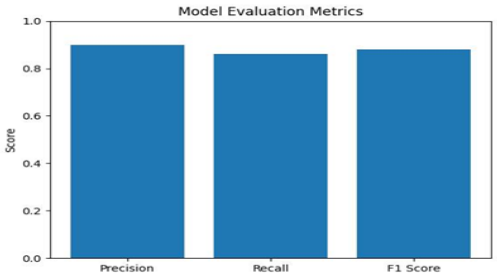



Fig 3: Evaluation Metrics

Confusion Matrix:

A Confusion Matrix is a table that is used to evaluate the performance of a classification model. The performance of a classification model is often evaluated by using a confusion matrix that compares the actual result with the result from the classification model.

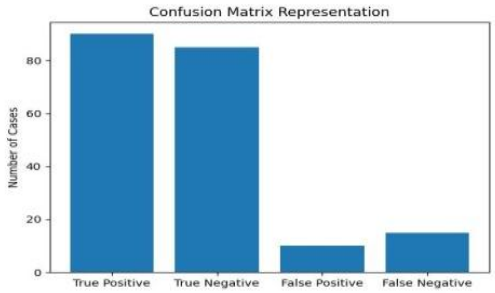



Fig 4: Confusion Matrix

C)Result

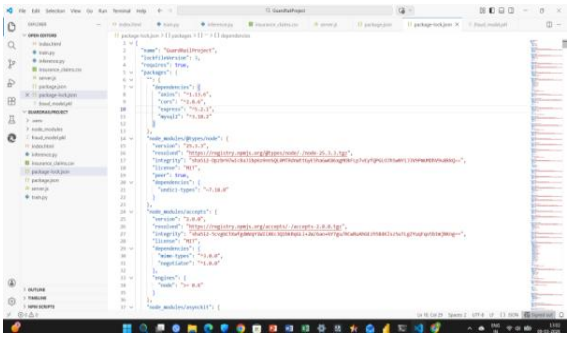


Fig 5: Frontend Code

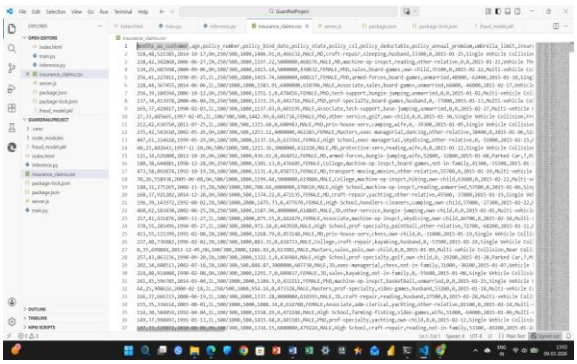


Fig 6: Dataset

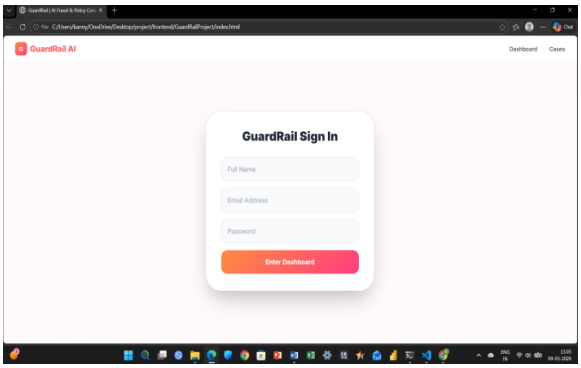



Fig 7: Login Page

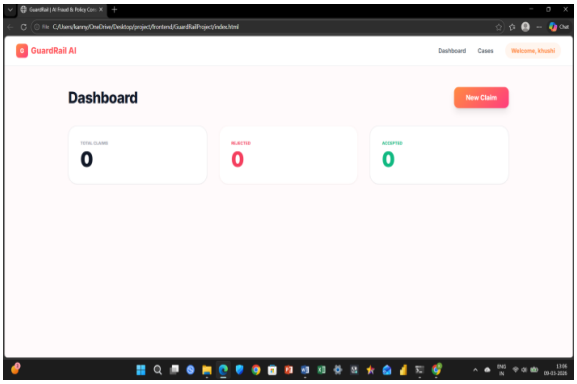



Fig 8: Output Dashboard

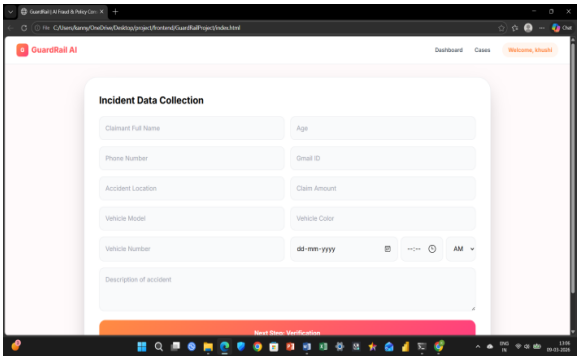



Fig 9: Index Page

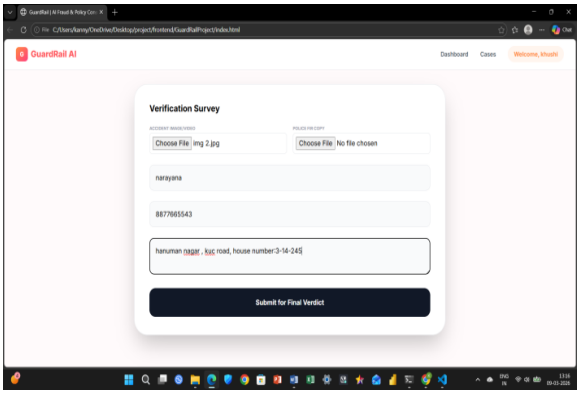



Fig 10: Verification Survey

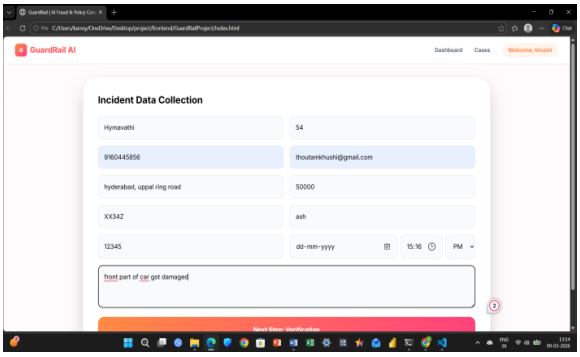



Fig 11: Data Collection

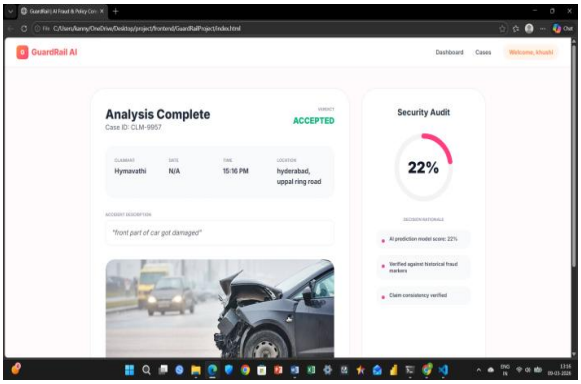



Fig 12: Final Result Analysis

## V. CONCLUSION

The Random Forest algorithm, praised for handling large data sets with many features and for its resistance to overfitting, is employed in insurance fraud detection where it examines claim amounts and customer histories to uncover suspicious patterns. Web-based AI-powered risk assessment platforms streamline the claims workflow by instantly delivering machine-learning generated scores that enable adjusters to quickly pinpoint high-risk claims. A typical machine-learning architecture couples a React front-end with a Node. js back-end for API handling, uses Flask as a lightweight framework to serve model predictions through REST calls, and stores claim data and fraud scores in MySQL, allowing micro-services to communicate in real time. Performance metrics used in the assessment of the performance of a model in distinguishing between fraudulent and genuine claims. A performance of over ninety percent in insurance fraud detection is considered effective.

## VI. FUTURE SCOPE

Guardrails AI enables developers to create reliable artificial intelligence systems, and research has demonstrated that modern techniques boost financial analysis precision by significant amounts. The system achieves operational success through its ability to modify guardrail settings according to user query patterns, while customer success teams implement artificial intelligence for risk assessment by studying multiple elements to improve their results. While there is significant latency for the first guardrail layer, there is minimal latency for the subsequent layers, which allows for multiple protection layers and ensures smooth operation for different artificial intelligence models. The system also ensures monitoring and development through its collection of guardrail events and measurement of latency and false positive rates, and its continuous improvement of accuracy assessment, which allows the model to learn and improve over time.

## REFERENCES

[1] "Automobile insurance fraud detection using machine learning techniques," Scientific Reports, 2025.

[2] "Machine learning techniques applied to insurance fraud detection systems," IEEE Xplore Digital Library, 2025.

[3] "Artificial intelligence framework for detecting fraud in insurance claims," IEEE Xplore Digital Library, 2025.

[4] "Machine learning approaches for identifying fraud in insurance systems," IEEE Xplore Digital Library, 2025.

[5] "Advanced machine learning models for insurance claim fraud detection," IEEE Xplore Digital Library, 2025.

[6] "Artificial intelligence techniques for detecting fraud in insurance claims," IEEE Xplore Digital Library, 2025.

[7] "Machine learning approaches for fraud detection in insurance systems," Computers, MDPI, 2025.

[8] "Mathematical models using artificial intelligence for insurance fraud detection," Mathematics, MDPI, 2025.

[9] "AI-based methods for fraud detection in insurance datasets," Electronics, MDPI, 2025.

[10] "Machine learning techniques for intelligent fraud detection systems," Applied Sciences, MDPI, 2025.

[11] "Artificial intelligence and machine learning for insurance fraud detection," Data Science and Analytics, Elsevier, 2024.

[12] "Artificial intelligence techniques for fraud detection in insurance systems," Applied Artificial Intelligence, Taylor & Francis, 2024.

[13] "Machine learning based insurance fraud detection system," IEEE Xplore Digital Library, 2024.

[14] "Data-driven fraud detection for insurance claims," IEEE Xplore Digital Library, 2024.

[15] "Fraud detection and analysis for insurance claims using machine learning," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 2024.