**Deep Learning Approaches for Detecting Fraudulent Claims in Medical Insurance**

**Mithilesh Vishwakarma1, Dr. Santosh Kumar Singh2, Niraj Jain3, Lalit Pal4**

1Assistant professor, Department of IT, Thakur College of Science and Commerce, Thakur Village,
Kandivali (East), Mumbai, Maharashtra, India

2H.O.D, Department of IT, Thakur College of Science and Commerce, Thakur Village, Kandivali (East), Mumbai, Maharashtra, India

3,4PG student, department of IT, Thakur College of Science and Commerce, Thakur Village, Kandivali (East), Mumbai, Maharashtra, India

1amitpandey8089@gmail.com, 2sksingh14@gmail.com, 3jainniraj40@gmail.com,

4lalitpal9969@gmail.com

**Abstract**

Fraudulent claims in medical insurance present a significant challenge to the healthcare system, leading to financial losses estimated to be in the billions annually. These fraudulent activities can take many forms, including billing for services not rendered, upcoding, and falsifying medical records. Not only do these practices inflate costs for insurers, but they also adversely affect genuine claimants and undermine the integrity of healthcare systems. As such, detecting and preventing fraud is crucial for maintaining trust and financial stability within the insurance industry

Traditional fraud detection methods often rely on rule-based systems and manual audits, which can be time-consuming and inefficient. In recent years, deep learning techniques have emerged as powerful tools for identifying fraudulent activities with high accuracy. This study explores the application of a Feed Forward Neural Network (FFNN) for detecting fraudulent claims in medical insurance. The proposed model is trained on historical claims data, utilizing key features such as claim amount, diagnosis codes, and patient history to differentiate between genuine and fraudulent claims.

Performance evaluation metrics, including accuracy, precision, recall, and F1-score, demonstrate the model's effectiveness in identifying suspicious claims. The results indicate that FFNN-based approaches can significantly enhance fraud detection accuracy compared to traditional methods, thereby improving efficiency and reducing financial losses in the insurance sector.

**Keywords**

Deep Learning, Fraud Detection, Medical Insurance Fraud, Feed Forward Neural Network (FFNN), Multilayer Perceptron (MLP), Machine Learning in Healthcare, Healthcare Data Analysis.

**1. Introduction**

Medical insurance fraud is a growing concern that results in significant financial losses for insurance companies, increased premiums for honest policyholders, and inefficiencies in the healthcare system. Fraudulent claims can take various forms, including billing for services not rendered, exaggerating medical conditions, and providing false information to receive higher reimbursements. Traditional fraud detection methods rely on manual audits and rule-based systems, which are often time-consuming, prone to errors, and unable to adapt to evolving fraudulent tactics.With the advancements in machine learning, automated fraud detection systems have emerged as a promising solution to identify suspicious claims more effectively. Machine learning techniques can analyze large volumes of claim data, detect hidden patterns, and flag potentially fraudulent activities with greater accuracy than conventional approaches. Among these techniques, the Random Forest algorithm has gained attention due to its ability to handle high-dimensional data, mitigate overfitting, and provide reliable predictions.

This study explores the application of machine learning, particularly the Random Forest algorithm, in detecting fraudulent medical insurance claims. By leveraging historical claim data and key features, the model can classify claims as legitimate or fraudulent, helping insurers streamline the claim verification process and reduce financial losses. The research focuses on data preprocessing, feature selection, model evaluation, and performance comparison with other machine learning techniques.The objective of this research is to demonstrate the effectiveness of machine learning-based fraud detection in medical insurance, emphasizing the advantages of Random Forest in improving accuracy, interpretability, and efficiency. The findings aim to contribute to the development of intelligent fraud detection systems, ultimately enhancing the security and reliability of medical insurance claims processing.

Machine learning (ML) has emerged as a powerful tool for detecting fraudulent claims in medical insurance. By leveraging vast amounts of historical claim data, ML models can identify suspicious patterns and anomalies that might go unnoticed by conventional detection methods. These models use advanced algorithms, such as decision trees, neural networks, and anomaly detection techniques, to classify claims as fraudulent or legitimate with high accuracy.

### **2. Literature Review:**

Fraudulent claims in medical insurance pose a significant challenge to insurance providers, resulting in financial losses and operational inefficiencies. Traditional fraud detection techniques often struggle to identify sophisticated fraudulent patterns, necessitating the adoption of deep learning approaches. Among various deep learning models, Feed Forward Neural Networks (FFNN) and Multilayer Perceptron (MLP) have gained attention for their ability to detect fraudulent claims efficiently. This section reviews existing studies on fraud detection in medical insurance using deep learning techniques, with a focus on FFNN and MLP.

Early fraud detection methods relied on rule-based systems and statistical analysis (Phua et al., 2010). These approaches used predefined rules, such as claim amount thresholds and unusual provider behavior, to flag suspicious claims. However, as fraudsters devised more sophisticated methods to bypass these rules, traditional approaches became inadequate.

Subsequent studies incorporated machine learning techniques such as decision trees, support vector machines (SVM), and logistic regression to improve fraud detection accuracy (Van Vlasselaer et al., 2015). While machine learning models outperformed rule-based systems, they required extensive feature engineering and struggled with high-dimensional data.Deep learning has emerged as a powerful tool for detecting fraudulent medical insurance claims by automatically extracting patterns from large datasets. Unlike traditional models, deep learning architectures such as FFNN and MLP can handle complex, high-dimensional data and identify subtle fraud indicators.

FFNN is a widely used deep learning model in fraud detection due to its ability to learn hierarchical representations of claim data. Studies have demonstrated that FFNN models outperform conventional machine learning techniques by detecting nonlinear relationships in fraud patterns. model's performance. Several studies have compared FFNN, MLP, and traditional machine learning models to determine the most effective fraud detection approach.

Wang et al. (2021) conducted a comparative analysis and found that deep learning models, particularly FFNN and MLP, outperformed logistic regression and random forests in detecting fraudulent medical claims.

Ahmed et al. (2022**)** highlighted that FFNN and MLP achieved higher accuracy and lower false positive rates, making them superior alternatives to rule-based fraud detection systems.

Key evaluation metrics used in these studies include:
Accuracy – Measures overall correctness of fraud classification.
Precision & Recall – Evaluate the model’s ability to identify fraudulent claims accurately.
F1-score – Provides a balance between precision and recall.

### **3. Methodology**

This study investigates deep learning approaches for detecting fraudulent claims in medical insurance, focusing on **Feed Forward Neural Networks (FFNN)** and Multilayer Perceptron (MLP). The methodology consists of several key steps, including data collection, preprocessing, model architecture, training, evaluation, and performance analysis.

**Data Collection and Preprocessing:**

**Data Preprocessing:** The dataset underwent cleaning, handling missing values, removing duplicates, and standardizing categorical features. Numerical features were scaled using StandardScaler. Categorical features were one-hot encoded.

* **Patient information:** Age, gender, medical history
* **Claim details:** Claim amount, type of treatment, frequency of claims
* **Provider information:** Hospital or doctor ID, location, specialization
* **Billing details:** Diagnosis codes, procedure codes, cost breakdown

**Model Development:** A deep learning model with two hidden layers (128 and 64 units) was constructed using Keras. ReLU activation was used for hidden layers, and sigmoid activation for the output layer.

**Training:** The model was trained using the Adam optimizer and binary cross-entropy loss function.

**Evaluation:** Model performance was assessed on a held-out test set using accuracy, precision, recall, F1-score, and AUC.

### **3.1 Dataset Description**

The dataset used for this study contains 1,000 records with 40 attributes, including both numerical and categorical features. The primary objective is to detect fraudulent medical insurance claims. Below is a summary of the key features and their significance:

### Key Observations:

* The dataset contains both numerical and categorical features, with a mix of continuous and discrete variables.
* There are no missing values in the primary columns except for the column named \_c39, which appears to contain only null values.
* The dataset shows a high variance in claim amounts and premiums, indicating the presence of both high and low-value claims.
* The **fraud\_reported** column serves as the target variable for classification.



*Figure 1. Dataset Overview*

### Data Quality and Preprocessing:

* Encoding categorical variables (e.g., **insured\_sex**, **insured\_education\_level**) will be necessary to apply machine learning models.
* Scaling and normalization of numerical features will be performed to ensure consistency.



### *Figure 2. Correlation Matrix of Features*

This correlation matrix helps in feature selection for machine learning models. Highly correlated features might be redundant, while uncorrelated features may contribute unique information. Based on this, variables like total claim amount, injury claim, property claim, and vehicleclaim could be strong predictors for fraud detection models.

### 4. **Experimental Results**:

The deep learning model developed in this experiment shows considerable promise for automated insurance fraud detection. Its high accuracy and robust performance suggest its potential for practical application in the insurance industry. Further research and development could further refine and enhance its capabilities.

**Key Findings:**

**High Accuracy:** The model achieved an **accuracy of 0.9750** on the test set, demonstrating its ability to correctly classify insurance claims as fraudulent or not.

**Strong Predictive Power:** High precision and recall scores indicate that the model effectively identified fraudulent claims while minimizing false positives and false negatives.

**Robustness:** The model exhibited good generalization performance, as evidenced by the ROC curve and Precision-Recall curve.

**Discussion:** The experimental results strongly suggest that the deep learning model is effective in predicting fraudulent insurance claims. The high accuracy and other evaluation metrics indicate that the model has learned relevant patterns from the data and can generalize well to unseen instances. This capability holds significant potential for automating fraud detection in the insurance industry.

**Further Analysis:** While the model demonstrates promising performance, future work could explore:

* **Hyperparameter Tuning:** Fine-tuning the model's hyperparameters could potentially further improve its performance.
* **Feature Engineering:** Exploring additional features or interactions between features might enhance the model's predictive power.
* **Model Interpretability:** Techniques like SHAP values or LIME could be used to understand the model's decision-making process and identify important features.

### 4.1 **Evaluation Metrics**

This section outlines the evaluation metrics used to assess the performance of the deep learning model in predicting fraudulent insurance claims.

**Accuracy:** Accuracy represents the proportion of correctly classified instances (both fraudulent and non-fraudulent) out of the total number of instances.

* Formula: Accuracy = (TP + TN) / (TP + TN + FP + FN)
* TP: True Positives (correctly predicted fraudulent claims)
* TN: True Negatives (correctly predicted non-fraudulent claims)
* FP: False Positives (incorrectly predicted fraudulent claims)
* FN: False Negatives (incorrectly predicted non-fraudulent claims)

**Precision:** Precision measures the proportion of correctly predicted fraudulent claims out of all claims predicted as fraudulent.

**Formula: Precision = TP / (TP + FP)**

**Recall (Sensitivity):** Recall measures the proportion of correctly predicted fraudulent claims out of all actual fraudulent claims.

**Formula: Recall = TP / (TP + FN)**

**F1-Score:** The F1-score is the harmonic mean of precision and recall, providing a balanced measure of the model's performance

**Formula: F1-Score = 2 \* (Precision \* Recall) / (Precision + Recall)**



*Figure 1. Model Accuracy*

By including the formulas for each evaluation metric, this section provides a clear and comprehensive understanding of how the model's performance was assessed. This level of detail enhances the transparency and reproducibility of our Paper. which allows readers to grasp the mathematical basis behind each metric and how it contributes to the overall evaluation of the model's effectiveness in predicting fraudulent insurance claims.

### **4.3 Visualizations**

1. **Confusion Matrix:**

****

*Figure 1. Random Forest Confusion Matrix*

1. **Receiver Operating Characteristics**

****

*Figure 2.Operating Characteristic*

1. **Model Recall Curve:**

**

*Figure 3.Precision - Recall Curve*

### **5**. **Limitations**

**1. Data Dependency:**

* **Limited Data:** Deep learning models typically require large amounts of data to train effectively. If the available dataset is limited, the model's performance might be affected, particularly its ability to generalize to unseen instances.
* **Data Bias:** If the training data is biased or does not accurately represent the real-world distribution of fraudulent and non-fraudulent claims, the model might exhibit poor performance on unseen data.

**2. Interpretability:**

* **Black Box Nature**: Deep learning models are often referred to as "black boxes" due to their complex internal workings. Understanding the reasons behind the model's predictions can be challenging, making it difficult to identify potential biases or areas for improvement.

**3. Overfitting:**

* **Complexity:** Deep learning models can be prone to overfitting, especially with complex architectures and limited data. Overfitting occurs when the model learns the training data too well and fails to generalize to new data.

**4. Adaptability:** Evolving Fraud Patterns: Fraudulent activities constantly evolve, and the model might need to be retrained regularly to adapt to new patterns and maintain its effectiveness.

**5. Feature Engineering:** The model's performance heavily relies on the quality and relevance of the features used. Identifying and engineering effective features are crucial steps in building a successful model.

Addressing these limitations through careful data preparation, model selection, evaluation, and monitoring can help build a more robust and reliable system.

### **5.**1 **Future Work**

A feedback neural network model has demonstrated a high accuracy of 97% in detecting fraudulent medical insurance claims, there remain several avenues for future exploration and enhancement.

1. **Model Optimization and Fine-Tuning:** While the current model achieves remarkable accuracy, further optimization techniques such as hyperparameter tuning and ensemble learning could enhance performance, particularly in more complex or unstructured datasets.
2. **Integration of Multimodal Data:** Incorporating additional data modalities, such as textual data from claim descriptions or patient records, could improve detection accuracy. Utilizing techniques like natural language processing (NLP) combined with the current feedback neural network model might yield richer insights.
3. **Real-Time Fraud Detection:** Implementing the model for real-time fraud detection is another potential area of development. Adapting the model for continuous learning and real-time data processing could significantly benefit insurance companies in promptly identifying and mitigating fraudulent activities.
4. **Explainability and Interpretability:** Deep learning models, particularly neural networks, often operate as black boxes. Enhancing model interpretability using techniques like SHAP (SHapley Additive exPlanations) or LIME (Local Interpretable Model-Agnostic Explanations) would increase stakeholder trust and help identify potential biases or inconsistencies in fraud detection.
5. **Transfer Learning and Domain Adaptation:** Applying transfer learning techniques to leverage knowledge from related domains could reduce the need for large training datasets. Additionally, domain adaptation techniques could make the model more robust when deployed in different geographic regions or insurance systems.
6. **Ethical and Privacy Considerations:** Addressing privacy concerns associated with using sensitive medical data is critical. Future work could focus on federated learning or privacy-preserving techniques to maintain data confidentiality while leveraging distributed data sources.

**6. Conclusion**

This project has successfully demonstrated the potential of deep learning for automated insurance fraud detection. Through careful data preprocessing, feature engineering, and model development, we have built a deep learning model that achieves high accuracy in predicting fraudulent insurance claims. The experimental results highlight the model's effectiveness in identifying fraudulent claims while minimizing false positives and false negatives.

The key findings of this project include:

* High Accuracy: The model achieved an accuracy of 0.9750 on the test set, demonstrating its ability to correctly classify insurance claims as fraudulent or not.
* Strong Predictive Power: High precision and recall scores indicate that the model effectively identified fraudulent claims while minimizing false positives and false negatives.
* Robustness: The model exhibited good generalization performance, as evidenced by the ROC curve and Precision-Recall curve.

These results underscore the potential for deep learning to revolutionize fraud detection in the insurance industry. By automating the process, insurance companies can significantly reduce the time and resources spent on manual investigations, while also improving the accuracy and efficiency of fraud detection. This can lead to substantial cost savings and a more secure insurance ecosystem. However, it is crucial to acknowledge the limitations of the current model, such as its dependence on data quality and potential for overfitting. Future work should focus on addressing these limitations through hyperparameter optimization, feature engineering, model architecture enhancements, and exploring explainability techniques.

Despite these limitations, the results of this project provide strong evidence for the effectiveness of deep learning in insurance fraud detection. With continued research and development, deep learning models can play a vital role in mitigating fraud and ensuring a more secure and trustworthy insurance industry.

### 7. References

1. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). "A Comprehensive Survey of Data Mining-based Fraud Detection Research." *arXiv preprint arXiv:1009.6119*.
2. Sadgali, I., Youssfi, M., & El Afia, A. (2019). "Machine Learning Techniques for Insurance Fraud Detection: A Review." *Procedia Computer Science*, 148, 148-156.
3. Ngai, E.W.T., Hu, Y., Wong, Y.H., Chen, Y., & Sun, X. (2011). "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature." *Decision Support Systems*, 50(3), 559-569.
4. Yuan, Y., & He, K. (2015). "An Improved Random Forest Model for Insurance Fraud Detection." *Journal of Financial Risk Management*, 4(3), 90-95.
5. Zhang, X., Zhang, Y., & Wang, L. (2018). "Fraud Detection in Insurance Claims Using Machine Learning Algorithms." *International Journal of Advanced Computer Science and Applications*, 9(6), 42-49.
6. Chauhan, A., & Gupta, B.B. (2019). "Application of Machine Learning in Healthcare Insurance Fraud Detection." *International Journal of Healthcare Information Systems and Informatics*, 14(1), 75-92.
7. Kou, Y., Lu, C.-T., Sirwongwattana, S., & Huang, Y.-P. (2004). "Survey of Fraud Detection Techniques." *IEEE International Conference on Networking, Sensing and Control*, 2, 749-754.