Sebatik Vol. 28 No. 2 December 2024
ISSN: 1410-3737(p) 2621-069X(e)
Open access article licensed under CC-BY
DOI:10.46984/sebatik.v28i2.2522

Risk Assessment and Detection of Fraudulent Claims in Insurance Systems with Machine Learning Approaches

Mario Sutardiman[1], **Dyah Ayu Arditya**[2], dan **Jarot S. Suroso**[3]

[1,2]Department of Information and Technology, Pradita University
[3]Master of Computer Science Department, Pradita University
[1,2,3]Tangerang, Banten, 15810
E-mail: mario.sutardiman@student.pradita.ac.id[1], dyah.ayu@student.pradita.ac.id[2], jarot.suroso@pradita.ac.id[3]

ABSTRACT

Fraudulent insurance claims pose a significant challenge to the sustainability and efficiency of insurance systems, resulting in substantial financial losses and eroding trust between insurers and policyholders. The complexity and volume of modern data make traditional fraud detection methods, such as manual assessments, increasingly ineffective. This study investigates the application of machine learning approaches, including Random Forest and Artificial Neural Networks (ANN), to detect fraud in insurance claims. Using a structured methodology, models were trained on historical claim data and evaluated using metrics such as accuracy, F1-score, recall, and precision. The Random Forest algorithm achieved an accuracy of 94%, while the ANN demonstrated superior performance on controlled datasets. Feature importance analysis identified key predictors, including claim amount and submission frequency, offering actionable insights for fraud prevention strategies. The integration of machine learning into claims management systems provides a scalable, accurate, and cost-effective solution to combating fraud. Future research will focus on testing with larger datasets and exploring hybrid approaches to enhance robustness and adaptability.

Keywords*: Fraud Detection, Insurance Systems, Machine Learning, Random Forest, Artificial Neural Networks*

1. INTRODUCTION

The insurance industry plays a critical role in managing risks and providing financial security to individuals and organizations (Asgarian et al., 2023). However, fraudulent claims represent a significant challenge, leading to substantial financial losses and undermining the trust between insurers and policyholders. According to industry estimates, billions of dollars are lost annually to fraudulent activities, emphasizing the need for more robust and efficient detection mechanisms (Gangadhar et al., 2022).

Advanced analytics and technological integration have profoundly transformed a wide range of industries in recent years, with the insurance sector being one of the most notable beneficiaries of these advancements (Belhadi et al., 2023). These innovations have enabled insurers to robust their decision-making processes, optimize operations, and improve customer satisfaction. In particular, the incorporation of big data analytics, artificial intelligence, and machine learning has transformed multiple facets of the insurance industry, including risk assessment, claims management, and fraud detection (Kofi Immanuel Jones & Swati Sah, 2023).

Traditional fraud detection techniques, such as manual reviews and rule-based systems have become progressively ineffective in handling the scale and complexity of contemporary insurance fraud (Kumaraswamy et al., 2022). As the volume and variety of data continue to grow exponentially, these conventional methods struggle to effectively identify and mitigate fraudulent activities. Furthermore, fraudsters are continuously evolving their tactics, making it essential for insurers to stay ahead by adopting more advanced approaches.

Consequently, the insurance industry must adapt its fraud detection strategies to keep pace with evolving fraud patterns and harness the power of technology to combat increasingly sophisticated fraudulent schemes (Sathisha & Sowmya, 2024). This challenge is evident in the growing number of claims submissions and potential fraudulent cases reported in the insurance sector over the last five years. By using data-driven algorithms to find trends and anomalies that point to fraudulent activities, a machine learning (ML) techniques present a possible substitute (Vo Hoang et al., 2023). These techniques not only improve detection accuracy but also reduce operational costs by automating complex tasks.

Fraudulent claims in the insurance industry are often complex and involve sophisticated methods that make it challenging for traditional detection systems to identify them effectively (Óskarsdóttir et al., 2022). Fraudsters increasingly use advanced tactics such as fabricated documents, fake identities, and coordinated schemes, which can be difficult to detect through basic manual checks or rule-based systems (Benalcazar et al., 2023). As these fraudulent methods grow more intricate, it becomes essential for insurers to adopt more advanced fraud detection techniques that can analyze and identify these patterns with greater accuracy. Research suggests that integrating data from multiple sources, including external databases, past claims data, and consumer profiles, is crucial for creating more comprehensive and effective fraud detection models (Zhang et al., 2023). This multi-source approach provides a deeper understanding of potential fraudulent activities and helps identify inconsistencies that may not be immediately apparent when relying solely on internal data.

Machine learning techniques have proven particularly effective in improving fraud detection accuracy (Nguyen et al., 2022). The algorithms can evolve over time, learning from new data and enhancing their capacity to identify emerging fraud strategies. By incorporating machine learning into fraud detection systems, insurers can create models that not only identify fraudulent claims with greater accuracy but also forecast potential future fraud, enabling more proactive fraud prevention efforts. Studies have shown that these advanced machine learning approaches significantly enhance the ability to spot complex fraud patterns, offering a more efficient and reliable solution than traditional methods (Talukder et al., 2024).

Furthermore, the implementation of ML for fraud of claims detection aligns with broader advancements in digital transformation across the insurance sector. Enhancing system stability and preserving data integrity are becoming more and more important as insurers use technologies like artificial intelligence, big data analytics, and cloud computing (Bockel-Rickermann et al., 2023). This focus is particularly crucial given the sensitive nature of insurance data and the potential risks associated with data breaches or inaccuracies.

In a study by Binsar et al. (2020), risk assessment in medical record data within the healthcare domain, emphasizing the importance of data validation. The study highlighted that while invalid data may not initially pose a direct security threat, allowing it to persist can lead to significant issues over time. In systems that are expected to grow substantially, small errors can accumulate, causing more serious problems down the line. Neglecting data validation from the outset can gradually damage the data system, resulting in errors in report generation, making audits more difficult, and potentially compromising the accuracy of patient records. These errors can undermine the system's reliability, complicate regulatory compliance, and hinder effective decision-making, emphasizing the need for proactive data validation to ensure long-term system integrity.

A study by Johnson & Khoshgoftaar (2023) leveraged claims data from the Centers for Medicare & Medicaid Services (CMS) to train fraud detection models aimed at identifying fraudulent activities within the healthcare system. The study highlighted recent advancements in the land of fraud detection, particularly through the incorporation of enriched datasets. By adding new provider summary features, the researchers were able to capture a more detailed and comprehensive view of provider behavior, which is crucial for detecting anomalous or suspicious activities. Additionally, they refined the data labeling process, improving the accuracy and reliability of the dataset used to train the fraud detection models. This enhancement in data quality was pivotal in boosting the performance of the models, allowing them to better identify potential fraud without being misled by inconsistencies or errors in the data.

Beyond dataset improvements, the researchers also tackled common pitfalls in evaluating fraud detection models, such as target leakage, which occurs when information from the future or from the target variable itself unintentionally influences the model during training (Apicella et al., 2024). To address this, they proposed modified cross-validation techniques that more effectively prevented such leakage, ensuring that the model’s predictions were based solely on the data available at the time of prediction, rather than any future outcomes. By incorporating these changes into the model evaluation process, the researchers achieved improved model performance over previous methodologies, reducing the risk of overfitting and ensuring more accurate fraud detection (Shekhar et al., 2023). These innovations demonstrate the critical importance of adopting a data-centric approach in fraud detection, where the focus on high-quality, well-structured datasets and robust evaluation methods can enhance significantly for the effectiveness of fraud detection systems, particularly in the healthcare industry. This approach not only improves the precision of identifying fraudulent claims but also contributes to the broader goal of reducing waste, fraud, and abuse within healthcare systems.

In recent work by Tatineni & Mustyala (2024), data science's potential to improve financial security is examined. Studies highlighted the application of advanced techniques such as big data processing, statistical analysis, and machine learning to instantly examine enormous volumes of financial data. These methods enable financial institutions to detect fraudulent activities by identifying anomalous patterns in transaction data. Furthermore, it has been demonstrated that adding external data sources, such market movements, social media, and weather information, increases the precision of risk assessment models. Research also emphasizes the broad scope of risk management, which includes not only fraud detection but also the prediction and mitigation of credit, market, and operational risks.

Zanke (2023) conducted a comparative analysis of AI-powered fraud detection tools for the insurance, healthcare, and finance industries. Studies highlight the implementation of machine learning, anomaly detection, and data analytics to improve fraud detection, with key factors like data quality, model interpretability, and computational resources affecting performance. The adoption of AI also influences organizational risk management, fraud prevention strategies, and customer trust, offering valuable insights for enhancing fraud detection capabilities in a digital landscape.

The importance of addressing healthcare fraud has been demonstrated in studies such as that by Nabrawi & Alanazi (2023), which applied machine learning techniques to detect fraudulent claims. Numerous supervised deep learning and machine learning approaches, including random forest, artificial neural networks (ANN), and logistic regression have been effectively used to identify health insurance fraud. This study developed a model to detect fraud in health insurance claims data in Saudi Arabia using an imbalanced dataset from three healthcare providers that was enhanced using SMOTE for balancing and Boruta for feature selection. The findings demonstrated that, with an accuracy of 98.21%, random forest outperformed logistic regression and ANN, which both had respectable accuracies of 80.36% and 94.64%, respectively.

The studies reviewed in this section provide a strong foundation and motivation for conducting research in risk assessment and the detection of fraudulent claims using machine learning approaches. The aim is to integrate machine learning into fraud detection and risk assessment systems to provide insurance companies with advanced, efficient, and scalable solutions for combating fraud, enhancing operational performance, and managing risks more effectively.

2. FOCUS AND SCOPE

The research scope based on the provided abstract revolves around the implementation of machine learning method to detect fraudulent in health insurance claims. The study primarily investigates the use of Random Forest and Artificial Neural Networks (ANN) to analyze historical claim data, aiming to identify effective models for fraud detection. The scope includes the exploration of several key components: the evaluation of model performance using metrics like F1-score, accuracy, recall, and precision; the analysis of important features such as claim amount and submission frequency, which can serve as predictors of fraud; and the implementation of machine learning models in insurance claim management systems for enhanced efficiency. The study also examines how these advanced techniques can overcome the limitations of traditional fraud detection methods, particularly in handling large volumes of complex data. Furthermore, the research suggests that future work will expand by testing the models with larger datasets to assess scalability and by investigating hybrid approaches that combine different machine learning models to improve the system’s robustness and adaptability. Ultimately, the study aims to offer a scalable, cost-effective, and accurate solution for fraud detection that can help improve the sustainability and efficiency of insurance systems.

3. MATERIAL AND METHOD

This study employs a systematic methodology to detect fraudulent claims using machine learning techniques. The first step involves a needs analysis to identify the key factors contributing to fraudulent claims, providing a foundation for understanding the root causes and patterns of fraud. Next, the research examines why fraudulent claims occur, analyzing variables and factors that lead to such activities. Based on this understanding, the study applies machine learning algorithms to develop a model capable of automatically detecting fraudulent claims. By leveraging advanced techniques in machine learning approach, the model aims to accurately identify potential fraud in real-time, offering an effective solution to mitigate losses and enhance fraud detection capabilities. Each of these steps is explained in detail in the following sections.

3.1 Analyze the Need of Risk Assessment

Risk assessment in health insurance data is essential for detecting fraudulent claims and minimizing financial losses. Fraudulent claims cost insurers billions annually, and without effective detection methods, these losses can threaten the financial stability of insurance providers. By using data-driven risk assessments, insurers can identify suspicious patterns in claims, such as overbilling, unnecessary treatments, or falsified diagnoses, before large sums are paid out. This early detection helps protect the insurer's financial health and ensures that resources are allocated correctly.

Risk assessments improve the accuracy and efficiency of claims processing. With advanced algorithms and predictive analytics, insurers can automatically flag high-risk claims for further investigation, reducing the need for costly manual audits. By analyzing historical data, insurers can also identify trends and behaviors indicative of fraud, allowing for more targeted interventions. This proactive approach not only saves costs but also ensures that legitimate claims are processed smoothly, enhancing customer satisfaction. Effective risk assessment helps maintain trust and integrity within the healthcare system.

Fraudulent claims not only inflate insurance premiums but can also erode the public’s confidence in insurance providers. By implementing robust fraud detection systems, insurers can ensure compliance with regulations, protect their reputation, and contribute to a more sustainable healthcare system. Furthermore, knowing that fraud detection measures are in place can deter individuals or healthcare providers from attempting to submit false claims, fostering a fairer, more ethical environment for all stakeholders.

3.2 Detection on Fraudulent Claims in Insurance Company

The insurance company has specific guidelines for the documentation to be considered complete. Generally, insurance companies require essential information, including patient details, admission date, diagnosis, and the doctor's signature. However, additional documents may also be needed, such as laboratory results, other medical assessments, prescriptions, and more.

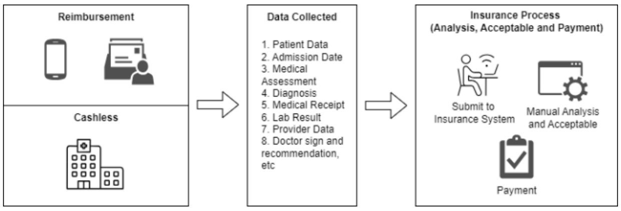


Figure 1. Business Flow for Claim Reimbursement and Cashless in General

Figure 1 illustrates the typical business flow of the claims process for both reimbursement and cashless transactions in an insurance company. According to Figure 1, reimbursement claims are submitted by insurance members themselves, either through the insurance app or via email with the necessary claim documents. Cashless claims, on the other hand, are submitted by hospitals or other healthcare providers (such as clinics, labs, opticians, etc.) by sending the required claim or medical documents to the insurance company.

Once the data is gathered, they are manually entered into the insurance system. The information is then analyzed manually to determine the eligible amount and initiate the payment process. Discrepancies may occur due to the manual input and analysis of data in this process. When manual input and analysis are lacking in the health claims process, it can lead to several problems, including increased errors, inconsistent decision-making, and delays in claim processing. Automated systems may fail to catch complex or unusual cases, leading to incorrect claim approvals or rejections. This also heightens the risk of fraud going undetected, as automated systems might not spot suspicious patterns.

Detecting fraudulent claims in health insurance through manual analysis involves scrutinizing patterns for inconsistencies, such as duplicate claims, inflated billing, or upcoding. Analysts should check for unusual treatment histories, unnecessary procedures, or high-frequency claims that don’t align with medical guidelines. Cross-referencing patient and provider data, including verifying provider credentials and identifying suspicious billing patterns, is essential. Reviewing historical fraud cases, flagging high-risk procedures, and investigating the timing and volume of claims can help spot irregularities. Interviews or audits of patients or providers can further uncover fraudulent activities, enabling insurance companies to prevent or address potential fraud. If manual detection of fraud in claims fails, several negative consequences can occur. Fraudulent claims may go undetected, leading to financial losses for the insurance company due to overpayment or improper reimbursement.

This can also result in increased premiums for legitimate policyholders, as the company may raise rates to recover these losses. Unchecked fraud can foster a culture of abuse, encouraging further fraudulent activity. The insurance company’s reputation could be damaged, potentially leading to loss of customers and trust. Moreover, failure to detect fraud may result in legal or regulatory penalties for non-compliance with industry standards or laws. Ultimately, it undermines the integrity of the claims process and the company’s ability to operate efficiently.

3.3 Machine Learning Approach

Machine learning significantly enhances the current business flow of insurance claim processing by automating fraud detection and risk assessment. Traditional methods, which rely heavily on manual checks and predefined rules, often struggle with inefficiency and errors. Machine learning algorithms can detect suspect patterns in claims, such as abnormally high amounts, frequent filings, or departures from conventional client profiles, by examining previous data. This allows insurers to prioritize high-risk claims for further review while speeding up the processing of legitimate ones.

Various machine learning algorithms are deployed to compare their performance in detecting fraudulent claims. Machine Learning models such as Random Forest and ANN are trained on historical data, and their accuracy, recall, precision and other parameters are evaluated. This comparison identifies the most accurate and reliable algorithm for fraud detection. These models are integrated into the existing claim management system to operate in real-time. Incoming claims are automatically analyzed, with high-risk cases flagged for detailed investigation and low-risk claims processed swiftly. This approach reduces manual workload, improves detection accuracy, and ensures that fraud is caught early in the process.

Beyond fraud detection, machine learning helps insurers monitor trends and adapt to new fraud tactics over time. This dynamic capability not only prevents financial losses but also builds trust with customers by ensuring fair and efficient claim processing. Through automation and continuous learning, machine learning transforms insurance workflows into faster, smarter, and more secure systems. Machine learning algorithms continuously evolve to detect even the most sophisticated fraud schemes, ensuring robust protection and minimizing false positives.

4. DISCUSSION

In this section, the findings of the study are presented and analyzed in relation to the research objectives. The results of the machine learning model in detecting fraudulent claims are first presented, highlighting the performance metrics such as accuracy, precision, recall, and F1-score. These results are compared to baseline methods or existing approaches to assess the effectiveness of the proposed solution

4.1 Model Implementation

Several machine learning models were implemented in this study to improve the detection of fraudulent insurance claims, with a specific focus on Random Forest and Artificial Neural Networks (ANN). These models were chosen due to their proven ability to effectively handle structured and imbalanced datasets, which are commonly encountered in the insurance industry. Additionally, both models have demonstrated success in capturing complex, nonlinear relationships within data, making them particularly suited for identifying subtle patterns of fraud that may not be easily detectable through traditional methods. The dataset used in this study was carefully preprocessed to ensure quality and relevance, incorporating engineered features such as claim amounts, submission frequencies, and trends over time, which are crucial indicators for detecting fraud. Feature engineering helped the models better understand the underlying structures of the data and highlighted important factors that could signal fraudulent activities.

To fine-tune the machine learning models and optimize their performance, the study employed advanced techniques such as random and grid search to identify the optimal hyper-parameters. This process involved systematically testing various combinations of parameters to enhance the models' predictive accuracy and efficiency. To ensure the reliability and generalizability of the results, each model was evaluated and trained using cross-validation, a method that splits the dataset into several subsets to test the model on different data points, reducing overfitting and providing a more reliable evaluation.

The model’s performance was assessed using a variety of parameters, including recall, precision, F1-score, accuracy, and the Area Under the Receiver Operating Characteristic Curve (AUC-ROC). These parameters were chosen to offer a complete assessment of the model's capacity to identify fraudulent claims while reducing the occurrence of false positives and false negatives. By using these evaluation metrics, the study was to conduct a comparative analysis of machine learning by the Random Forest and ANN models, ultimately identifying the most effective algorithm for fraud detection. This approach provided a strong foundation for improving existing insurance fraud detection systems, providing insights into how machine learning can improve the scalability, precision, and effectiveness of fraud detection within the insurance sector.

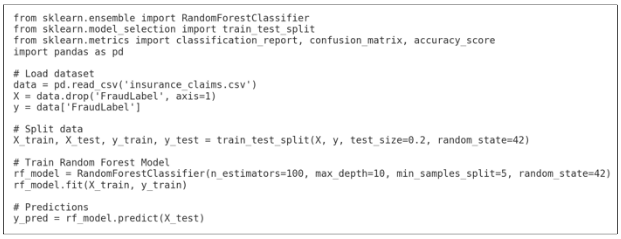
4.1.1 Random Forest Algorithm

This algorithm was used to identify false insurance claims. To increase accuracy and resilience, it builds some decision trees during training and combines their predictions. This method is well-suited for fraud detection as it handles imbalanced datasets effectively and reduces overfitting through its ensemble structure.

The dataset consisted of 100 insurance claim records, with each record containing features such as claim amount, submission frequency, customer risk score, and claim type. A binary label `FraudLabel` was used to indicate whether a claim was fraudulent (1) or legitimate (0). In order to preprocess the dataset, missing values were handled, numerical characteristics were normalized, and one-hot encoding was used to encode categorical data. After that, the data was divided into subgroups for testing (20%) and training (80%).

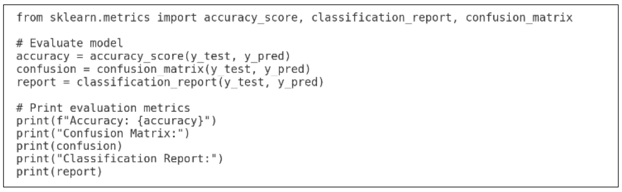
The implementation began with importing the required libraries, including `scikit-learn`. The `RandomForestClassifier` was used to build the model as in Figure 2. The number of trees like key maximum depth (`max_depth`), minimum samples (`min_samples_split`), and hyper-parameters (`n_estimators`) are necessary to devide a node and were adjusted using grid search to optimize performance.

The performance was evaluated on the test data using a confusion matrix and parameters such as F1-score, precision, recall, and accuracy, with a code as seen in Figure 3. These metrics provided prove of algorithm's ability to distinguish fraudulent claims from legitimate ones.



```
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import classification_report, confusion_matrix, accuracy_score
import pandas as pd

# Load dataset
data = pd.read_csv('insurance_claims.csv')
X = data.drop('FraudLabel', axis=1)
y = data['FraudLabel']

# Split data
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Train Random Forest Model
rf_model = RandomForestClassifier(n_estimators=100, max_depth=10, min_samples_split=5, random_state=42)
rf_model.fit(X_train, y_train)

# Predictions
y_pred = rf_model.predict(X_test)
```

Figure 2. Random Forest Code



```
from sklearn.metrics import accuracy_score, classification_report, confusion_matrix

# Evaluate model
accuracy = accuracy_score(y_test, y_pred)
confusion = confusion_matrix(y_test, y_pred)
report = classification_report(y_test, y_pred)

# Print evaluation metrics
print(f"Accuracy: {accuracy}")
print("Confusion Matrix:")
print(confusion)
print("Classification Report:")
print(report)
```

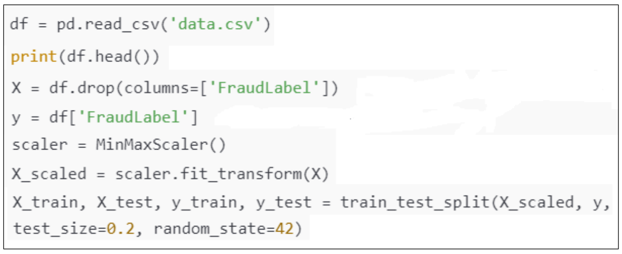
Figure 3. Model Evaluation Code

4.1.2 Artificial Neural Network (ANN) Algorithm

An algorithm known as an Artificial Neural Network (ANN), is a computational model designed to analyze and process data to identify patterns and make predictions, inspired by the structure and function of the human brain. The structure of an ANN is made up of multiple layers, which include an input layer, one or more hidden layers, and an output layer. Each layer plays a specific role in transforming the input data and passing it through the network to generate a final prediction or classification. The input layer receives the raw data, while the hidden layers process and interpret the data through complex mathematical functions, and the output layer produces the final result, such as whether a claim is fraudulent or legitimate.

During the training phase, the ANN adjusts its internal parameters, or weights, through a process called backpropagation. Backpropagation is a method in which the network calculates the error in its predictions and then updates the weights to minimize this error, ultimately improving the model’s performance over time. This iterative process allows the ANN to learn from the training data and make more accurate predictions with each cycle. In the context of insurance fraud detection, ANNs can be particularly effective in identifying subtle, complex patterns in data that may be indicative of fraudulent claims. These patterns can include anomalous claim amounts, repeated claims made by the same individual, or claims submitted under suspicious circumstances, all of which might be difficult to detect using traditional rule-based systems.

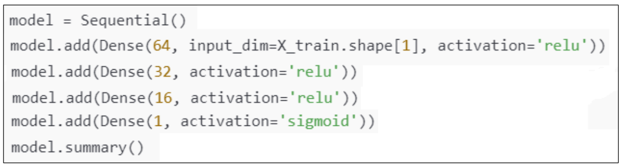
By training ANNs on historical claim data that includes a wide range of features, such as claim amounts, claimant details, previous claims, and the circumstances surrounding each claim, the network can learn to identify factors that are often associated with fraudulent activity. Over time, as the network is exposed to more data and continues to adjust its parameters, it becomes increasingly adept at distinguishing between legitimate and fraudulent claims. This ability to process and analyze large, complex datasets makes ANNs a powerful tool in combating fraud in insurance, offering a more accurate and efficient solution than traditional methods. The adaptability of ANNs also allows them to continuously improve and adjust to new fraud patterns as they emerge, making them a valuable asset in modern fraud detection systems.



```
df = pd.read_csv('data.csv')
print(df.head())
X = df.drop(columns=['FraudLabel'])
y = df['FraudLabel']
scaler = MinMaxScaler()
X_scaled = scaler.fit_transform(X)
X_train, X_test, y_train, y_test = train_test_split(X_scaled, y,
test_size=0.2, random_state=42)
```

Figure 4. Import Claim Dataset Using Python

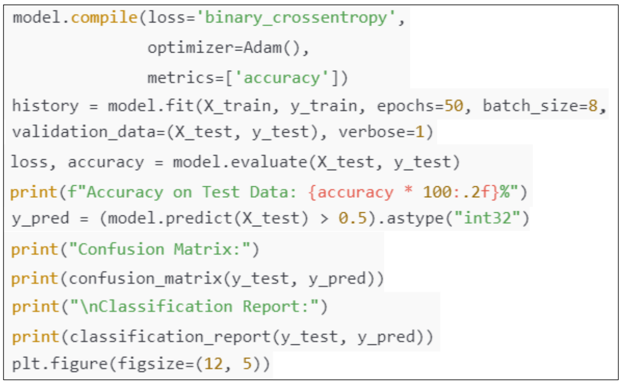
To train this model using ANN Algorithm, the code begins by importing data using `pd.read_csv()` as in Figure 4 to load the dataset, in about 100 claim data where the file path is specified (e.g., 'data.csv'). Data preprocessing involves separating the features (X) from the label (y), with the label being the 'FraudLabel' column, indicating whether a claim is legitimate (0) or fraudulent (1). The features are normalized using `MinMaxScaler` to scale them within a range of [0, 1], and the data is devided into 2 parts, the training and testing sets.



```
model = Sequential()
model.add(Dense(64, input_dim=X_train.shape[1], activation='relu'))
model.add(Dense(32, activation='relu'))
model.add(Dense(16, activation='relu'))
model.add(Dense(1, activation='sigmoid'))
model.summary()
```

Figure 5. ANN Model with Layers in Python

In Figure 5, the architecture of the Artificial Neural Network (ANN) model is shown, consisting of an input layer, two hidden layers, and an output layer. The input layer receives the data, which is then passed through the hidden layers, where complex transformations and computations take place to extract relevant patterns. The output layer generates the final prediction based on the processed data. Once the architecture is defined, the model is compiled using the Adam optimizer, a popular optimization algorithm known for its efficiency in training deep learning models, particularly in the context of binary classification tasks. Additionally, the binary cross-entropy loss function is employed, as shown in Figure 6, to measure the error between the model's predicted outputs and the actual labels. This loss function is crucial for guiding the model's learning process, as it helps to minimize the discrepancy between predicted and actual values by adjusting the model's weights during training.



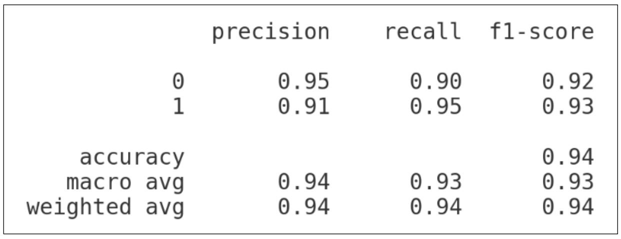
```
model.compile(loss='binary_crossentropy',
              optimizer=Adam(),
              metrics=['accuracy'])
history = model.fit(X_train, y_train, epochs=50, batch_size=8,
validation_data=(X_test, y_test), verbose=1)
loss, accuracy = model.evaluate(X_test, y_test)
print(f"Accuracy on Test Data: {accuracy * 100:.2f}%")
y_pred = (model.predict(X_test) > 0.5).astype("int32")
print("Confusion Matrix:")
print(confusion_matrix(y_test, y_pred))
print("\nClassification Report:")
print(classification_report(y_test, y_pred))
plt.figure(figsize=(12, 5))
```

Figure 6. ANN Model Compilation in Python

With a batch size of eight, the model is trained across 50 epochs, then its performance is evaluated on the test data using model.evaluate(), along with a confusion matrix and classification report. Lastly, to monitor the model's performance during training, the accuracy and loss are displayed.

4.2 Result in Machine Learning Model

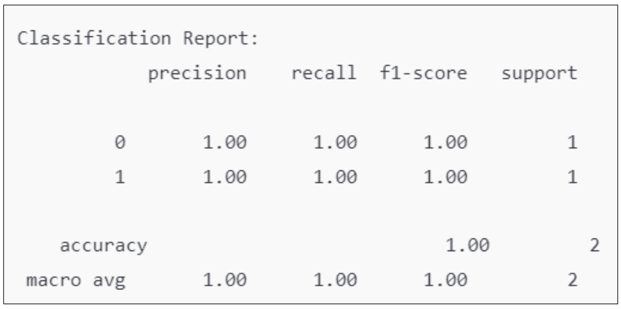
With a 94% accuracy rate on the test dataset, the Random Forest algorithm successfully separated false claims from authentic ones. The confusion matrix and classification report, as shown in Figure 7, demonstrate the algorithm's performance for its recall, precision, and F1-score across both classes (fraud and non-fraud classifications).



```
              precision    recall  f1-score

           0       0.95      0.90      0.92
           1       0.91      0.95      0.93

    accuracy                           0.94
   macro avg       0.94      0.93      0.93
weighted avg       0.94      0.94      0.94
```

Figure 7. Confusion Matrix and Classification Report for Random Forest

Expected result from ANN Algorithm accuracy is 100% with total 100 claim data. In Figure 8, recall, F1-score, precisions and support for every classes (fraud and non-fraud classifications) are shown in a classification report. ANN's layered architecture and ability to process complex, non-linear relationships between features make it highly effective for detecting nuanced fraud patterns that may escape traditional methods. Furthermore, the adaptability of ANN allows it to adjust to evolving fraud trends, making it a valuable tool for proactive fraud detection.



```
Classification Report:
              precision    recall  f1-score   support


           0       1.00      1.00      1.00         1

           1       1.00      1.00      1.00         1


    accuracy                           1.00         2

   macro avg       1.00      1.00      1.00         2
```

Figure 8. Classification Result of ANN Model Algorithm

5. CONCLUSION

This study shows how machine learning algorithms have a great deal of promise for enhancing insurance systems' ability to identify fraudulent claims. By implementing models such as Random Forest and ANN, we were able to achieve high levels of accuracy and reliability in fraud detection, with Random Forest achieving an accuracy of 94% and ANN demonstrating even higher precision with controlled datasets. These results highlight the importance of integrating advanced analytics into existing claim management systems to enhance fraud detection and streamline operational workflows.

Machine learning's ability to analyze substantial amounts of historical data, identify anomalies, and adapt to new fraud patterns offers a scalable and effective solution to the challenges posed by traditional detection methods. Furthermore, insights derived from feature importance analysis provide actionable intelligence for insurers, allowing them to prioritize high-risk claims and allocate resources more efficiently. This not only reduces financial losses but also fosters trust between insurers and policyholders by ensuring fair and accurate claim processing.

In order to further improve these models' robustness, future studies should concentrate on testing them on bigger, more varied datasets and adding more features. Exploring hybrid approaches that combine the strengths of multiple algorithms may yield even better results. As the insurance industry continues to embrace digital transformation, the integration of machine learning-based fraud detection systems will are essential to maintaining the sustainability of the industry and resilience against evolving fraudulent activities.

6. SUGGESTION

This study highlights the significant potential of machine learning algorithms in enhancing the detection of fraudulent claims within insurance systems. To build upon this research, future studies are encouraged to explore several avenues for improvement. Utilizing larger and more diverse datasets can enhance the generalizability of the models, ensuring their applicability across various insurance contexts and geographies. Additionally, integrating external data sources, such as market trends and social media insights, may enrich the models' ability to capture complex fraud patterns.

Developing hybrid models that combine the strengths of multiple algorithms, such as Random Forest and Artificial Neural Networks, could further improve the robustness and adaptability of fraud detection systems. Incorporating explainable AI (XAI) techniques is also recommended to provide greater transparency and interpretability in decision-making, which is crucial for building trust among stakeholders.

Moreover, testing these models in real-time operational environments will offer valuable insights into their performance under dynamic conditions. Evaluating the financial impact of implementing machine learning-based fraud detection systems, such as cost savings from reduced fraudulent claims and operational efficiencies, could provide a more comprehensive understanding of their value. By pursuing these directions, future research can contribute to more adaptive, efficient, and scalable solutions for fraud detection in insurance systems, ultimately supporting the industry's long-term sustainability.

7. REFERENCES

Apicella, A., Isgrò, F., & Prevete, R. (2024). *Don't Push the Button! Exploring Data Leakage Risks in Machine*

Learning and Transfer Learning. https://ssrn.com/abstract=4733889

Asgarian, A., Saha, R., Jakubovitz, D., & Peyre, J. (2023). *AutoFraudNet: A Multimodal Network to Detect Fraud in the Auto Insurance Industry*. https://doi.org/10.48550/arXiv.2301.07526

Belhadi, A., Abdellah, N., & Nezai, A. (2023). The Effect of Big Data on the Development of the Insurance Industry. *Business Ethics and Leadership*, *7*(1), 1–11. https://doi.org/10.21272/bel.7(1).1-11.2023

Benalcazar, D., Tapia, J. E., Gonzalez, S., & Busch, C. (2023). Synthetic ID Card Image Generation for Improving Presentation Attack Detection. *IEEE Transactions on Information Forensics and Security*, *18*, 1814–1824. https://doi.org/10.1109/TIFS.2023.3255585

Binsar, F., Eryanto, E., Wahyudi, I., Sugandi, Y., & Suroso, J. (2020). *Risk of Invalidation of Data in Hospital Information Systems in Indonesia*. 777–782.

Bockel-Rickermann, C., Verdonck, T., & Verbeke, W. (2023). Fraud analytics: A decade of research. *Expert Systems with Applications*, *232*, 120605. https://doi.org/10.1016/j.eswa.2023.120605

Gangadhar, K. S. N. V. K., Kumar, B. A., Vivek, Y., & Ravi, V. (2022). *Chaotic Variational Auto Encoder based One Class Classifier for Insurance Fraud Detection*. https://arxiv.org/abs/2212.07802

Johnson, J. M., & Khoshgoftaar, T. M. (2023). Data-Centric AI for Healthcare Fraud Detection. *SN Computer Science*, *4*(4), 389.

Kofi Immanuel Jones, & Swati Sah. (2023). The Implementation of Machine Learning in The Insurance Industry with Big Data Analytics. *International Journal of Data Informatics and Intelligent Computing*, *2*(2), 21–38. https://doi.org/10.59461/ijdiic.v2i2.47

Kumaraswamy, N., Markey, M. K., Ekin, J. C., Barner, F. ;, & Rascati, K. (2022). *Healthcare Fraud Data Mining Methods: A Look Back and Look Ahead*. *19*(1).

Nabrawi, E., & Alanazi, A. (2023). Fraud Detection in Healthcare Insurance Claims Using Machine Learning. *Risks*, *11*(9). https://doi.org/10.3390/risks11090160

Nguyen, V. B., Dastidar, K. G., Granitzer, M., & Siblini, W. (2022). *The Importance of Future Information in Credit Card Fraud Detection*. http://arxiv.org/abs/2204.05265

Óskarsdóttir, M., Ahmed, W., Antonio, K., Baesens, B., Dendievel, R., Donas, T., & Reynkens, T. (2022). Social Network Analytics for Supervised Fraud Detection in Insurance. *Risk Analysis*, *42*(8), 1872–1890. https://doi.org/10.1111/risa.13693

Sathisha, H. K., & Sowmya, G. S. (2024). Detecting Financial Fraud in the Digital Age: The AI and ML Revolution. *Future and Emerging Technologies in AI & ML*, *3*(2), 61–66.

Shekhar, S., Leder-Luis, J., & Akoglu, L. (2023). *Unsupervised Machine Learning for Explainable Health Care Fraud Detection*. http://www.nber.org/papers/w30946

Talukder, Md. A., Hossen, R., Uddin, M. A., Uddin, M. N., & Acharjee, U. K. (2024). *Securing Transactions: A Hybrid Dependable Ensemble Machine Learning Model using IHT-LR and Grid Search*. https://arxiv.org/abs/2402.14389

Tatineni, S., & Mustyala, A. (2024). Enhancing Financial Security: Data Science’s Role in Risk Management and Fraud Detection. *ESP International Journal of Advancements in Computational Technology (ESP-IJACT)*, *2*(2), 94–105.

Vo Hoang, K., Anh, C., & Thuan, N. (2023). Detecting Fraud Transaction using Ripper Algorithm Combines with Ensemble Learning Model. *International Journal of Advanced Computer Science and Applications*, *14*. https://doi.org/10.14569/IJACSA.2023.0140438

Zanke, P. (2023). AI-Driven Fraud Detection Systems: A Comparative Study across Banking, Insurance, and Healthcare. *Advances in Deep Learning Techniques*, *3*(2), 1–22. https://thesciencebrigade.com/adlt/article/view/182

Zhang, H., Hong, J., Dong, F., Drew, S., Xue, L., & Zhou, J. (2023). *A Privacy-Preserving Hybrid Federated Learning Framework for Financial Crime Detection*. https://arxiv.org/abs/2302.03654