

An Explainable AI Framework for Automated Medicare and Medicaid Claims Validation, Anomaly Detection, and Improper Payment Risk Assessment

Md Shakil Islam¹, Nishat Margia Islam²

¹Masters of Science in Business Analytics Trine University, USA

²Master of Science in Information Technology Washington University of Science & Technology, USA



DOI : <https://doi.org/10.61796/ipteks.v3i4>



Sections Info

Article history:

Submitted: July 20, 2026

Final Revised: August 11, 2026

Accepted: September 16, 2026

Published: October 08, 2026

Keywords:

Healthcare

Reimbursement

Medicare

Medicaid

Artificial Intelligence

Payment Risk

Dataset Provider-level

Fraud

ABSTRACT

Objective: This research aims to explore the patterns of healthcare claims, provider behaviour, and possible signs of payment risk using an explainable artificial intelligence approach that leverages the exploratory data analysis method. **Method:** Secondary data, including beneficiary, provider, inpatient, and outpatient claim data, were analyzed to look at distribution, relationships, and provider-level differences. Various descriptive statistical methods, comparative analyses, correlation assessment, and visual analytics were utilized to investigate reimbursement activity, claim frequency, beneficiary characteristics, and indicators of fraud. **Results:** The results show that providers with fraud indicators are a small fraction of the data set, but that there are significant differences in billing/reimbursing practices between this group and the rest of the providers. While the demographic variables show less correlation regarding payment patterns, there are meaningful correlations identified between the claim volume, reimbursement measures, and fraud indicators. Integrated anomaly analysis also identifies provider profiles that have unique claim and reimbursement patterns that could indicate that the provider is potentially underutilizing the program and could benefit from further administrative review. The study shows that explainable visual analytics can enhance the understanding of atypical billing patterns, potential claims validation issues, and provider-level payment risk characteristics, while not necessarily making fraud decisions. **Novelty:** The research highlights the importance of transparency, interpretability, and responsible handling of health care data, providing an analytical tool that can assist healthcare administrators, auditors, and researchers in analyzing intricate health care payment data and pinpointing areas for additional study.

INTRODUCTION

Background of Study

Healthcare insurance programs play a vital role in ensuring financial support for those who are eligible, and they need reliable systems for claim processing and reimbursing healthcare providers. In 2023, the Centers for Medicare and Medicaid Services (CMS) issued supplemental improper payment information that underscores the need to review the accuracy of payments in Medicare administration [1]. Medicare and Medicaid claims contain a myriad of records, including those of beneficiaries, health care services, provider activity, and reimbursement amounts. Issues with documentation or billing may make payments difficult and could cause problems for the administrators tasked with ensuring program integrity. Improper payment measurement is an important element in Medicare Fee-for-Service (FFS) payment monitoring efforts, as described in the 2023 FFS report. All of these concerns point to the need for analytical approaches that identify and consider the characteristics of claims and discover patterns

that warrant additional study. Exploratory data analysis provides a structured approach to comparing claim distributions, analyzing reimbursement variation, and exploring potential associations between provider characteristics and fraud indicators available. Visualizations can help clarify data sets and can help facilitate clear conversations regarding unusual observations and potential payment risks. In this study, Medicare claims data are analyzed to look for interpretable patterns that can be used to validate claims and for provider-level risk assessment.

Explainable AI in Healthcare Claims Validation and Fraud Detection

The application of Explainable Artificial Intelligence in healthcare fraud analysis can help explain analytical decisions to investigators and healthcare administrators. Muhammad et al. analyzed graph neural networks and explanation methods to detect suspiciousness in complex medical insurance claims data [2]. Their work shows how explanations can make relations between providers, patients, diagnoses, and medical services visible that affect model predictions. When claims are identified by automated systems, some of this transparency is relevant, as reviewers must have reasons that can be understood before they decide whether or not to pursue further investigation [2]. Furthermore, it must not be confused with proof of fraudulent activity as unusual patterns could also be indicative of legitimate differences in healthcare needs. . Visualizations can serve as a way to gain easy interpretation of the distributions of claims, reimbursements, and provider characteristics in exploratory research without it being asserted that the predictions have been put into practice. From an explainable AI perspective, this study investigates patterns that will be observed and their possible significance for claims validation and risk assessment for improper payments.

Problem Statement

Healthcare claims data is complex and may include relationships between beneficiaries, providers, diagnoses, medical services, and reimbursement records, which makes it challenging to consistently interpret claims that might be suspicious. Another peer-reviewed study in 2026 suggested an explainable machine learning model for healthcare fraud detection and emphasized the need for having transparent decisions in claims analysis [3]. While there are models that can detect suspicious provider behavior, their utility can be partly subject to the ability of investigators to comprehend the factors that lead to flagged records. The same research combined machine learning and blockchain evidence management, along with blockchain feature explanations, to increase transparency and auditing [3]. The development of a complete predictive framework, however, may involve the development of models, evaluation of the model performance, and provision of the supporting infrastructure that are not part of an exploratory study. The Medicare data set chosen includes beneficiary, inpatient, outpatient, and provider information, which can be analyzed using a structured visual analysis. Thus, this study tackles the question of whether meaningful distributions, relationships, and provider-level patterns can offer insights into possible claims irregularities and interpretable payment risk indicators. The study is based on evidence

that is exploratory and not conclusive or substantive enough to be considered evidence of fraud or other improper payments [3].

Research Objectives

- To analyze and compare the distribution and characteristics of healthcare claims, reimbursement amounts, beneficiary profile, and provider reimbursement behaviour to detect irregularities in claims validation and payment behaviour.
- To examine how relationships between the characteristics of claims, provider billing patterns, and available indicators of fraud or risk can be used to identify interpretable features that could assist in assessing improper payment risk within an explainable AI framework.

Research Question

What can an exploratory data analysis and explainable AI visualizations of Medicare claims data show about unusual billing trends, possible claims validation mistakes, and providers' risk of improper payment?

Significance of Study

This study is important because it looks at the potential of claims data to be used in a more transparent analysis of healthcare claims billing patterns and possible claim payment irregularities. Its visualizations can support researchers in grasping the variations in reimbursement amounts, characteristics of providers, and available fraud signs. The results could help health care administrators and auditors identify unusual patterns to investigate. The study highlights the importance of responsible conversations regarding explainable AI in healthcare payment analysis, through its focus on interpretable evidence. In addition, its exploratory approach offers a basis for future research with predictive models, case-level explanations, and validated indicators of improper payments. The results reported here, however, do not necessarily represent patterns across Medicaid programs, as they are based on the selected dataset, which is predominantly Medicare claims. The study thus provides an exploratory approach with a focus on prudent interpretation and the need for human verification prior to any payment and any decision related to fraud.

Artificial Intelligence in Healthcare Claims Processing and Fraud Detection

As the number of transactions and the complexity of reimbursement processes rises, healthcare claims processing has come under more scrutiny as insurers and public healthcare programs handle an increasing number of claims. Adepu [4] outlines an AI-powered payment architecture that leverages claims validation, predictive analytics, anomaly detection, natural language processing, and pattern recognition. The proposed solution suggests that automated verification should be linked to the fraud detection and reimbursement processes, suggesting that this should be done in conjunction with other processes as opposed to standalone applications. The article, however, does not report on an empirical evaluation of the project, but rather focuses on the conceptual design of the project and the description of potential benefits. It also demands real-time processing and interoperability, which adds to the requirements for its implementation beyond just

algorithm selection. The framework provides a valuable architectural view, but the improvements in accuracy and financial protection predicted will need to be tested with real claims data and operational results.

The challenges of modernization in public healthcare administration are increased by having to exchange claims information between systems while maintaining consistency and facilitating effective investigations. Fragmented enterprise data and lack of interoperability may limit claims analytics and the performance of traditional fraud prevention methods, according to Saha et al. [5]. They talk about modernization and interoperable data exchange, predictive analytics, anomaly detection, and explainable AI. This expanded institutional view builds on Adepu's payment processing model, focusing on infrastructure that can be used to enable analytical integration between Medicare and Medicaid systems. Furthermore, a sophisticated system is no more complete than the data it relies upon, and can't fix inconsistencies caused by incomplete data, unclear data definitions, or inaccurate fraud classifications. Therefore, the usefulness of modernization relies on the quality of the data, and the capacity to understand the results of the analysis in administrative terms. In exploratory research, these concerns reinforce the need for considering pattern at the dataset level, relationships between these patterns and repeatable suspicious activity before interpreting the patterns as suspicious activity at the provider level.

On the operational side, medical billing automation tackles repetitive management duties that have an impact on the quality of coding, claim acceptance, and reimbursement efficiency. Kilanko [6] explores how AI can be applied in the medical field to interpret patient records, suggest billing codes, minimize coding inaccuracies, and detect fraud and unusual transactions among healthcare providers. While Adepu's approach is based on an integrated payment design, this approach is more about dealing with billing processes and the implications of automation on administrative burden. Kilanko also recognizes issues with privacy, algorithmic bias, infrastructure, and employee training, which show that it is not an inevitable outcome of efficiency to be carried out responsibly. The article, however, does more than just examine Medicare provider fraud in a detailed manner; it provides an overarching international perspective. The arguments thus give scope for interpreting the elements of billing automation, without being conclusive evidence with regard to which aspects of the provider's characteristics or reimbursement variables set the unusual claims apart from the rest in a particular public healthcare program. This distinction is important for analyzing existing claims distributions prior to making specific analytical recommendations.

A more methodologically specific approach can be found in Hassan and Alam [7], where a hybrid method of supervised classification and unsupervised anomaly detection in healthcare claims processing is presented. They analyzed 1,200 claims that were anonymized, and examined the outcomes of approval, diagnostic details, procedural information, patient demographics, and billing patterns. Labelled classification and anomaly detection are crucial due to the fact that known fraud indicators and previously

unrecognized anomalies are separate challenges. However, the described data and model are not sufficient to make generalizations to large Medicare administrative data or to verify that all identified anomalies are fraud. While the conceptual discussion of system modernization provides a more abstract analysis, the approach provides a more concrete analytical design, but with limitations on its applicability depending on the representativeness of the data sets, the nature of the outcomes, and the validation procedures. Its focus on billing patterns makes it ideal for analysis of distributions and variable relationships, and the exploratory nature of its design means that it does not claim to be predictive of performance that has not been tested.

Additionally, the quantitative approach put forth by Sayem et al. [8] also takes into account AI-driven fraud prevention through secondary data analysis and statistical analysis of healthcare fraud. They explore the challenges of traditional manual audits and rule-based methods, and examine how AI can be used to detect fraudulent activity. This focus complements Hassan and Alam's claims processing framework, linking analytical automation with financial loss and healthcare system security issues. However, Sayem et al. mention several technological uses, such as voice biometrics, that could be different from the structured providers and reimbursement information found in Medicare claims. Thus, the facts are understood based on the methods and data analyzed, not applied to all healthcare fraud detection environments. The same analytical problem persists across these studies: how to interpret the patterns one sees in one's data without "noise" and how to differentiate between patterns one detects and noise. A practical way to explore this challenge without the assumptions about predictive modelling is to examine both provider labelling and claim frequency, as well as distributions of reimbursements and characteristics of the beneficiaries.

Medicare and Medicaid Claims Validation and Improper Payment Risk

A key tool to ensure that public healthcare finances are paid correctly and on program is healthcare claims validation. Claims might have inaccurate service codes, inaccurate patient data, duplicate charges, unsupported procedures, or amounts that need to be examined for reimbursement. Obviously, these irregularities don't necessarily mean there is intentional fraud, as administrative mistakes, missing documentation, and varying clinical situations can create unusual billing patterns. Kumaraswamy et al. [9] conducted a review of the methods employed for healthcare fraud data mining and pointed out the need to study various analytical methods used in detecting potentially fraudulent claims. Their review serves as a good basis for the importance of data analysis in healthcare payment monitoring. But spotting suspicious behavior is just one aspect of the process of validation. Effective review also involves the investigator following up on unusual patterns at the provider level and determining whether the evidence of the claim(s) is sufficient to warrant further investigation. This is key because an analytical system can detect an unusual billing pattern but not determine if there is an improper payment.

When payment systems in healthcare handle big volumes of claims from various beneficiaries, providers, and types of services, the challenge is further complicated. Nasir et al. [10] discussed anomaly detection using AI in United States government healthcare payment systems, particularly disbursements that could be considered improper and beneficiary misuse in federal public welfare programs. Their work is representative of the use of anomaly detection to detect payment patterns that would likely not be discovered during normal, manual review. However, caution must be taken when interpreting the anomalies that are detected. A beneficiary with above-average service use, or a provider with above-average reimbursement, could be due to legitimate differences in the nature of the services used, their specialization, or the beneficiaries served. For this reason, it is important to take into account the context of a claim when assessing the risk of paying out rather than the unusual values or statistical deviations. AI-driven anomaly detection methods have the potential to uncover more intricate patterns compared to traditional data mining techniques, but their utility relies on the quality of the data at hand and the need to provide explanations for the identified anomalies.

More recently, architectures creating the combination of different analytical methods for enhancing the understanding of billing discrepancies have also been investigated. Puli [11] suggested a hybrid system combining a large language model with graph-based analysis to detect inconsistencies in laboratory billing and possible overpayments. The proposed design links relationships between entities and billing information, which can be used to examine related claims, instead of each transaction as a separate record. The work, however, proposes an architecture that needs to be empirically validated and therefore effectiveness is not assumed as a fact. Patibandla [12] studied the context-aware detection of anomalies in a multi-stage decision pipeline. This puts into perspective the importance of integrating the context and iterative analytical evaluations rather than relying on a single detection phase. While each of these strategies has a different technical design, both indicate a need to consider healthcare payment irregularities across multiple sources of evidence. However, their use still requires adequate and accurate data regarding claims, providers, beneficiaries, and service conditions. Conclusions as to the cause or seriousness of an observed irregularity will remain limited if such contextual variables are not available.

Another point of view is that of unsupervised learning, which can discover strange payment observations without the need to have every claim be labeled as fraud. This work on unsupervised learning for anomaly detection in payment data from Australian health care providers is relevant to the study of healthcare reimbursement patterns. This study on unsupervised learning for anomaly detection in Australian medical payment data is a relevant comparison for medical payment data anomaly detection research. Unsupervised methods, which do not require labelled examples, can help to investigate previously unobserved differences in payment behavior. However, if an observation is recognized as being unusual, it should not be considered fraudulent or improper. There

are also important differences between the payment systems used in Australia and Medicare and Medicaid in the United States that reduce the extent to which this can be applied directly. These findings are consistent with the need for an exploratory investigation of Medicare claims, reimbursement distribution, provider-level variations, and fraud indicators. When the available variables and labels in the dataset allow it, interpretable visualizations can help reveal patterns that warrant further exploration or consideration. This type of analysis can be used for claims validation and claims payment-risk assessment, but should not be used to claim fraud or to prove the effectiveness of a trained predictive model.

Explainable AI, Anomaly Detection, and Transparent Risk Assessment

Explainable AI is a crucial aspect of intelligent risk assessment as it provides insights into how automated systems assess suspicious behavior and recognize potential threats. Anomaly Detection is the process of recognizing deviations from the behaviour of a transaction, operation, or a network of business systems in financial services, healthcare, and interconnected business systems. Sugumar [14] reviews an explainable AI framework that integrates financial, transactional, network, and textual data to explore the risks of financial fraud and cyber-enabled pharmaceutical network risks. The integration of multimodal analytics takes anomaly identification beyond the individual data attributes and also looks at the relationships between different types of information sources. These relationships, however, are not necessarily interpretable in the same way that the underlying models are capable of being detected. While explainable AI can offer human-readable explanations for predictions, the value of these explanations will depend on how accurate they are in approximating model actions and how relevant they are to the risk being explored. This separation emphasizes the connections between the recognition of deviant patterns and the formation of an accessible framework for the sense-making of their possible meaning.

Explainability also has a broader relationship with organisational decision-making in the use of data driven analytical approaches. Parameshwarappa et al. [15] define data-driven decision making as analytical techniques used to understand, interpret, and inform an organization's decisions. Topics discussed in the book include transparent AI-supported insights, automated fraud detection, and AI model security in financial and accounting analytics. These themes link analytical transparency to the interpretation of new and emerging risks, especially when decisions are based on complex data and multiple organisational objectives. However, data-driven decision-making and explainable AI are two different ideas. Data-driven approaches highlight the need to use data in a decision process, while explainable AI puts a stronger emphasis on the explanation of the algorithmic output. Therefore, the abundance of analytical details alone cannot be used to determine the understandability of the reasoning behind a model or to determine if the model's predictions could be used to support a specific risk classification.

Anomaly detection also assumes greater importance in the context of continuous monitoring, compliance assessment, and threat detection in cybersecurity auditing. Goswami [16] examines how to leverage Artificial Intelligence and Machine Learning in cybersecurity audits quantitatively by surveying 245 cybersecurity professionals from multiple industries. The results indicated positive relations between machine learning-based threat detection and high detection accuracy and between explainable AI and high auditor trust in automated results. The results relate algorithmic assessment, technical detection performance and organisational acceptance of algorithmic assessments. The ability to detect, however, can be different from its interpretability and trust. A model is able to find suspicious activity without giving an auditor an adequate description of the activity for classification. Likewise, the trustworthiness of a prediction is not proven by itself. The cross-sectional survey design of the study also limits its ability to determine detection performance across changing threat scenarios by reporting assessments from professionals and statistical relationships rather than direct experimental verification.

Transparent analytics and financial risk assessment come into play in cloud native enterprise resource planning (ERP) environments. Kräuterwald [17] discusses the applications of AI and machine learning in financial risk optimization in the context of financial systems in healthcare ERP systems, linking computational analytics with enterprise financial processes. This context is different from Sugumar's [14] multimodal fraud detection framework and Goswami's [16] cybersecurity auditing perspective, where enterprise risk optimization is about interpretation of the enterprise's financial and operational information in the integrated enterprise system. Distributed data sources, connected applications, and varying operating contexts are only a few of the analytic challenges that cloud native environments bring. However, these explainability techniques and anomaly detection metrics or empirical validation procedures are not specifically provided in the literature cited in [17]. In each of these research settings, interpretability of the analyses and the evidence to judge algorithmic classifications is still linked strongly with transparency of risk assessment.

Literature Gap

The existing literature has focused on AI-based claims validation, anomaly detection, fraud identification, and explainable risk assessment. Moreover, there is minimal incorporation of these perspectives with exploratory analysis of Medicare and Medicaid claims data. Exploration of provider-level differences, payment distribution, beneficiary characteristics, and fraud indicators can help explain non-traditional provider payment trends while not necessarily suggesting fraudulent activity or predictive capability.

METHODOLOGY

Research Design

This research study uses a quantitative exploratory approach to examine the area of healthcare claims validation, anomaly detection, and improper payment risk assessment in the context of healthcare data related to Medicare and Medicaid. The study aims to examine trends across provider characteristics, beneficiary data, inpatient and outpatient claims, and reimbursement variables. Exploratory Data Analysis (EDA) is an analysis method that is applied to look at distributions, variations, and relationships between the available variables without building and testing a predictive Machine Learning Model. This design enables the description of potential indicators of fraud and the separation of a group of statistically unusual observations from an observation of fraud. The analytical approach corresponds to the objectives of the study and explores patterns that are interpretable in the context of claims irregularity and provider-level risk characteristics.

Data Source and Description

The data set used in the study is the secondary data named "Healthcare Provider Fraud Detection Analysis" by Zhou and available from Mendeley Data. The data set has four CSV files: Train_Beneficiarydata.csv, Train.csv, Train_Inpatientdata.csv, Train_Outpatientdata.csv [18]. The files are used for information about beneficiaries, healthcare providers, and inpatient and outpatient claims. This information is used together to examine healthcare utilization, reimbursement trends, claim characteristics, and provider fraud indicators. The beneficiary file includes demographic and healthcare-related information, and the inpatient and outpatient files include information about the claims [18]. The provider-related file provides data that can be used to compare provider groups. These variables are available to make exploratory comparisons across healthcare payment records.

Data Preprocessing

Before analysis, the four CSV files are first checked for values that are missing, duplicate, inconsistent in data type, and irregular in variable formats, and this is referred to as data preprocessing. Beneficiary, provider, inpatient, and outpatient records are reviewed individually to learn about the structure of each and find appropriate variables for analysis. These ties are made using provider and beneficiary identifiers, consistency of date fields, and checking for consistency across numerical reimbursement variables. Where required, data for categorical variables (including provider fraud indicators) are standardized to allow for meaningful comparisons. Only meaningful record linkage will occur in data integration where there are compatible identifiers and relationships. The preprocessing step also filters out values that are not available, rather than replacing them with zero values, which could otherwise lead to misinterpreting the distribution of reimbursements and the volume of health care utilization.

Exploratory Data Analysis

Exploratory data analysis involves analyzing the distribution of provider fraud indicators, claims frequency, reimbursement amounts, beneficiary characteristics, and

comparing inpatient and outpatient services. Descriptive Statistics provide a summary of a numerical variable using measures of central tendency (mean, median, range) and dispersion. Frequency distributions can be used to analyse categorical data and illustrate various provider types. Comparative analysis is used to compare variations in reimbursement activity and claims activity for the available categories; the correlation analysis investigates correlations among selected numerical variables. Extreme reimbursement values and unusual observations are looked at as analytical indicators, not evidence of improper payments. These procedures are used to gain an exploratory understanding of the data and facilitate pattern identification for claims validation and provider-level risk assessment.

Visualization Strategy

The visualization strategy involves presenting healthcare claims information graphically to convey the distribution and relationships among such information. Providers' available fraud indicators are depicted in bar charts, and reimbursement amounts and claims characteristics are compared among similar providers using boxplots. The distribution and concentration of reimbursement values are displayed in histograms and relationships between selected numerical variables are investigated using scatterplots. An overview of associations between numerical claims and reimbursement characteristics is given in a correlation heat map. An integrated visualization merges selected provider-level indicators to allow for multiple dimensions of possible payment risk to be compared. The visualizations are created in RStudio with appropriate graphing packages: ggplot2 is used where appropriate. The variable(s) are understood in the context of each figure and the patterns seen in the figures' analysis.

Ethical Considerations

The research is secondary data without the recruitment of any participants or the collection of any new personal data. Ethical issues involve managing data responsibly, interpreting the data correctly, and avoiding false claims regarding healthcare providers or beneficiaries. Where present in the source files, identifiable information is not included in visualizations or descriptions published by the Bureau of Economic Geology. Provider fraud indicators are used as documentation of the meaning of these indicators in the dataset and not as independent evidence of fraudulent behavior. The analysis also acknowledges that there can be legitimate medical services coverage variations, beneficiaries' needs, provider specialization, or administrative factors that result in unusual claims and reimbursement patterns. Findings are reported at an appropriate analytical level, taking into account the confidentiality of the data, context of the findings, and the difference between suspected irregularities and verified improper payments.

Limitations

The limitations of the study are the structure, completeness, and representativeness of the selected secondary data. The indicators of provider fraud available may not detect all types of healthcare fraud or fraudulent payments, and data gaps and discrepancies in beneficiary and claims records may impact comparisons. In addition, some inpatient and

outpatient services can differ, which may affect reimbursement distributions and make it challenging to make apples-to-apples comparisons among providers. Also, statistical correlations and odd occurrences are no proof of any causal links or fraud. The analysis does not cover the development, training or validation of a predictive machine learning model, and therefore is unable to achieve predictive accuracy, generalization performance or operational effectiveness. The results are specific to the data set used and the variables that were recorded, and thus cannot be directly extrapolated to other healthcare payment systems or administrative systems.

Conceptual Framework

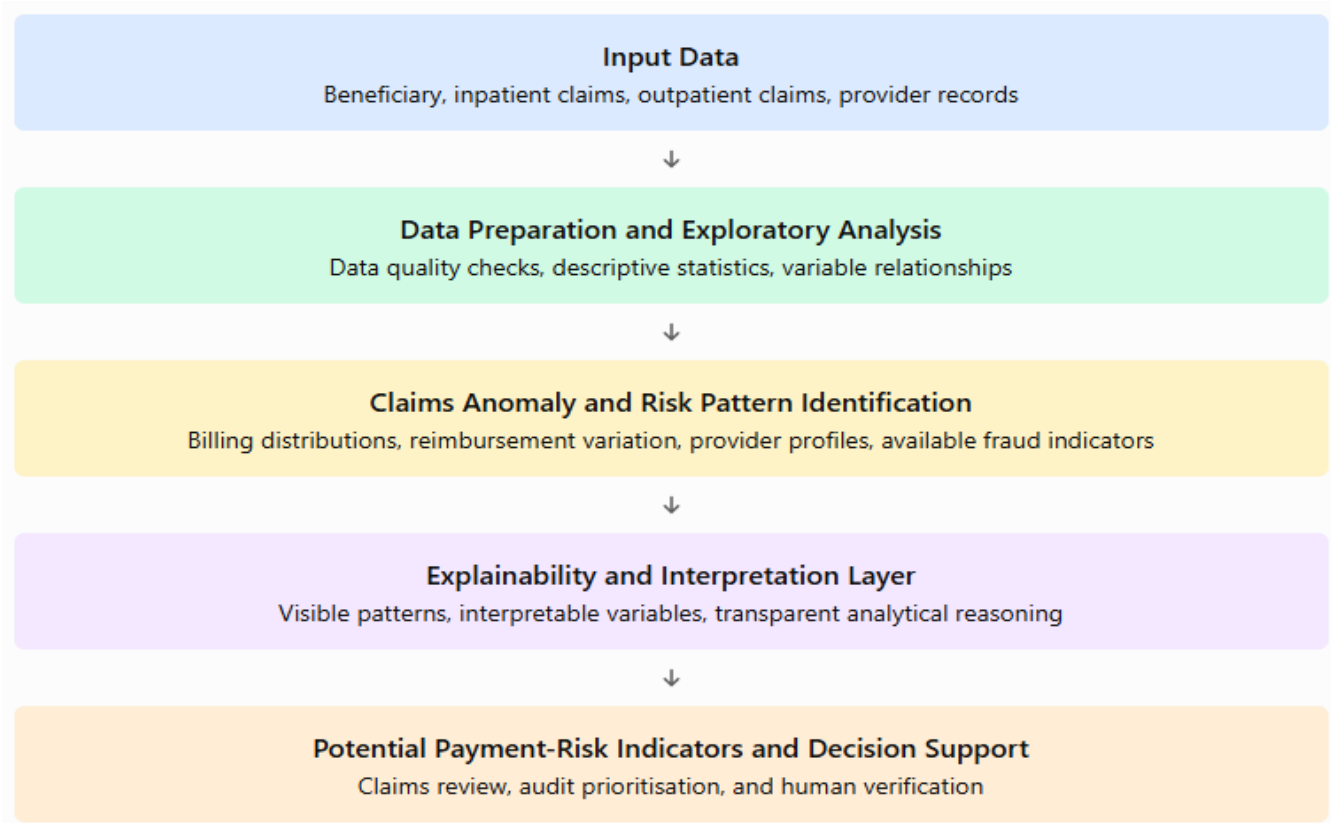


Figure 1. Conceptual Framework Diagram
(Source: Created by learner)

RESULTS

Distribution of Medicare Claims and Provider Fraud Indicators

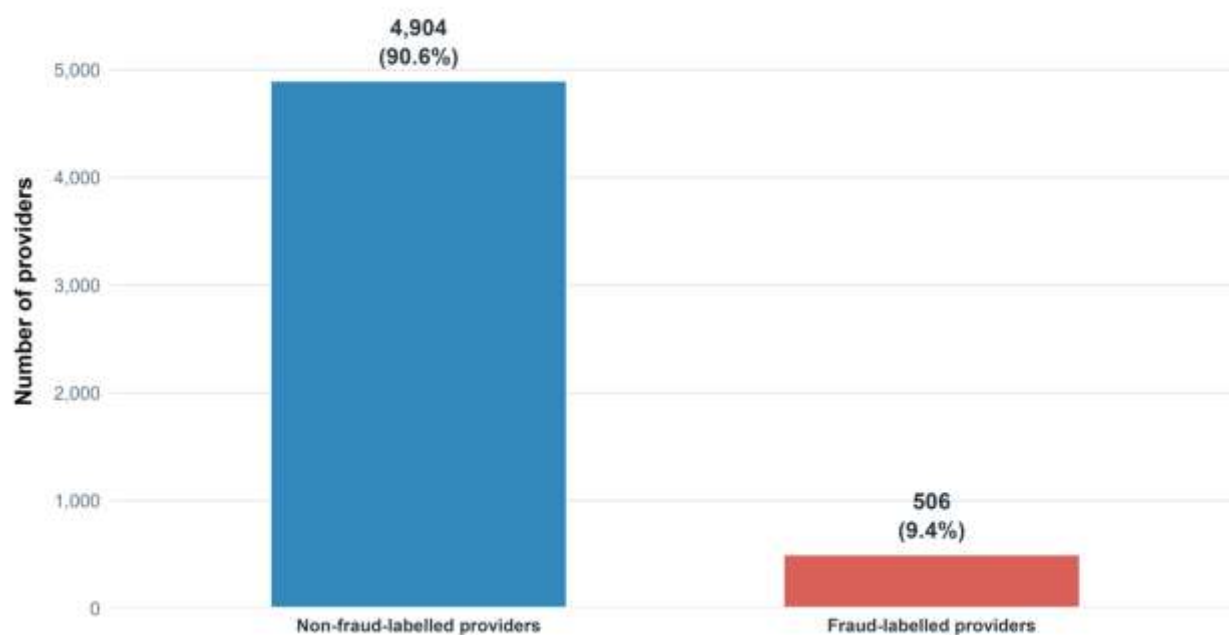


Figure 2. Provider Counts and Percentage of Analysed Records

(Source: Created by learner)

The distribution of providers is highly uneven, with 4904 providers (90.6 per cent) classified as non-fraud labelled and 506 providers (9.4 per cent) classified as fraud labelled. This pattern means that the behaviour of providers is unusual and is found in a smaller percentage of the dataset. The contrast emphasizes the need to look at the differences between providers, rather than simply at the overall number of claims. This differentiation can offer a basis for determining patterns linked with possible payment irregularities and reimbursement issues.

Claims and Reimbursement Patterns across Provider Groups

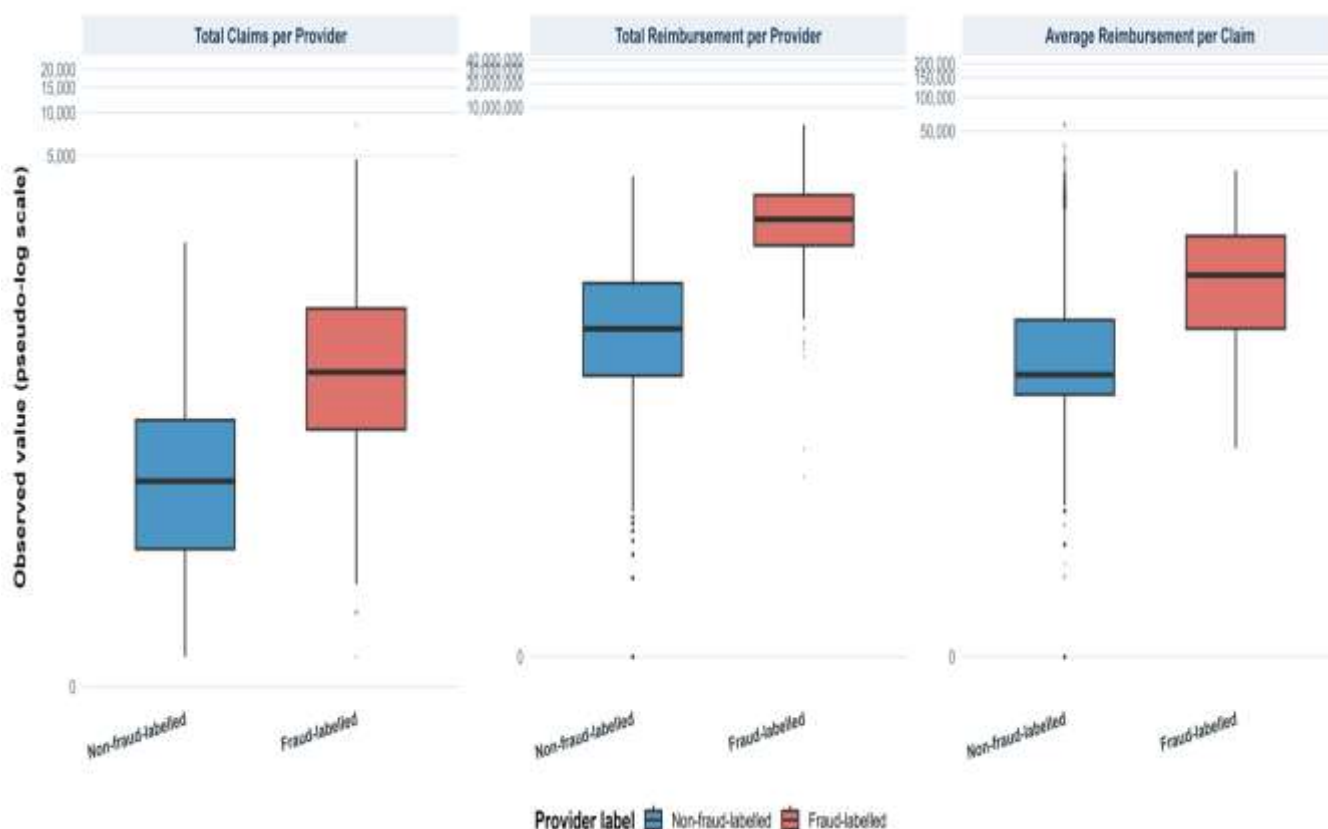


Figure 3. Provider-Level Comparison of Claim Volume and Reimbursement Using Inpatient and Outpatient Records

(Source: Created by learner)

There are clear differences in the claim activities and reimbursement behaviour of provider groups as shown in Figure 3. Providers labeled fraud have higher median claim amounts and higher total and median reimbursement amounts than non-fraud-labeled providers. The increased central tendency and wider distribution indicate that reimbursement concentration climbs with claim activity for these providers. These differences show important disparities in billing practices and payment results between provider types, and show reimbursement features that deserve more in-depth analysis in the claims validation process.

Relationships between Claims Characteristics and Potential Payment Irregularities



Figure 4. Pearson Correlations Across Claims, Reimbursement, and Beneficiary Indicator

(Source: Created by learner)

There are a number of robust relationships between the claims reimbursement and the beneficiary-related variables, as seen in Figure 4. Providers with more service and payment activity have more moderate positive relationships with inpatient claims total reimbursement and total claims, respectively, as seen in Figure 1, with fraud label. The total reimbursement is closely tied to inpatient claims and unique beneficiaries, indicating that growth in reimbursement is tied to both reach and volume of services. In contrast, there are comparatively low relationships between most variables and the age of the beneficiary and the chronic burden. Utilization and reimbursement factors play a more prominent role in explaining observed payment risk patterns.

Integrated Provider-Level Anomaly Patterns and Interpretable Improper Payment Risk Indicators

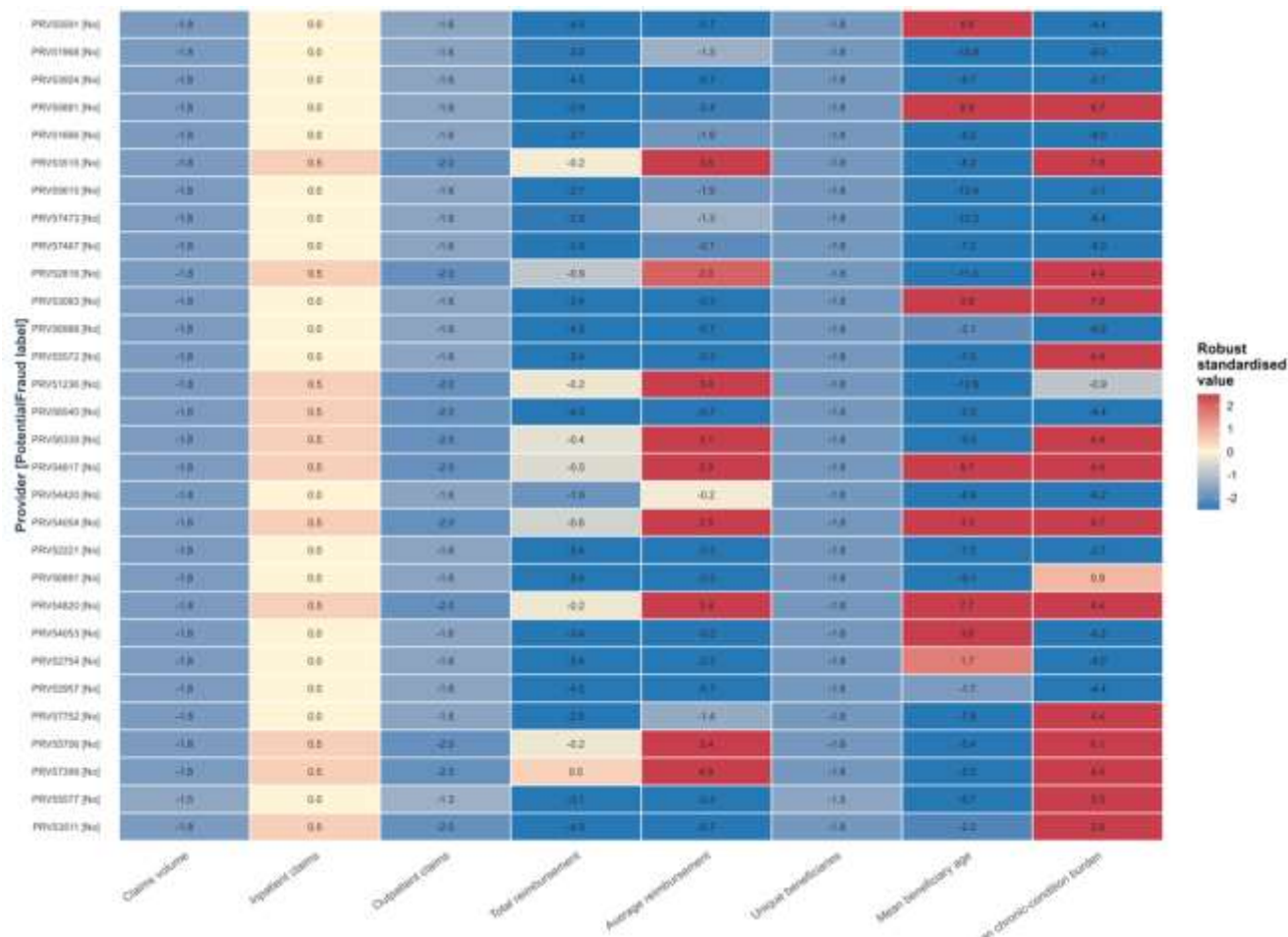


Figure 5. Thirty Most Unusual Provider Profiles Based on Multiple Claims (Source: Created by learner)

The 30 most unusual provider profiles based on multiple claim and reimbursement indicators are shown in Figure 5. The heatmap shows clear differences between providers; some providers have higher reimbursement indicators, whereas others have unique characteristics of their claims or beneficiaries. A combination of multiple indicators helps to identify more nuanced provider patterns that are not apparent from any one metric. This multi-dimensional approach enhances the understanding of irregularities with regard to payments.

Analysis of Results

The exploratory data analysis and explainable AI visualizations offer valuable insights into the Medicare claims data and its billing patterns. As shown in the figure, the distribution of providers showing fraud indicators indicates that a small share of providers has fraud labels and a larger share have non-fraud labels. This indicates that high levels of potentially problematic billing behaviour are not evenly distributed throughout the healthcare system and are likely to be focused on a small number of

providers. The discovery reflects the importance of analytical review, especially when provider groups are compared, to be able to see unusual patterns. The evidence presented here suggests that administrative monitoring may be enhanced by paying attention to provider characteristics rather than to aggregate claim volume.

Comparing the number of claims and the behaviour of claim reimbursement also shows significant differences among provider types. Providers with fraud indicators have higher claim activity and higher reimbursements than those without. These patterns indicate that higher billing activity may be associated with higher payment accumulation. This is reinforced by the correlation analysis as it can be observed that there are significant positive correlations between the reimbursement values, the claim frequency and the fraud indicators. Demographic factors like age and chronic condition burden seem to be less related to suspicious patterns at the same time. This illustrates that provider billing behavior and reimbursement activity provide better clues for analytical investigation than do attributes of the beneficiaries themselves. This means that visualizations can be used to pinpoint areas that could benefit from further investigation for claims validation efforts, as they often show higher levels of payment activity and claim intensity.

The integrated provider anomaly analysis provides the broadest possible view of improper payment risk. The visualization brings together several claim reimbursement and beneficiary-related measures to highlight providers with a profile that is very different from the rest of the dataset. These peculiarities are not necessarily a sign of fraud or any errors in payments, but merely flag providers whose billing practices should be examined in detail. The results proved to address the research question by showing that uncommon billing patterns can be identified, characteristics linked to potential claims validation issues can be highlighted, and provider profiles can be identified that exhibit increased payment risk characteristics through exploratory analysis and explainable visualizations. The study demonstrates the potential of healthcare claims data for evidence-based evaluation of irregular payment behaviour and a careful and explainable analytical approach.

Future Work

This study could be further extended by including sophisticated machine learning and explainable artificial intelligence models to analyze healthcare claims in more detail in the future. A predictive model can be created to determine if the identified reimbursement and claim patterns are associated with a better ability to detect unusual payment behaviour that is unusual. Explainability methods can be combined with classification and anomaly detection techniques to give clear reasoning about the outcomes of the analysis. These advancements could help healthcare administrators and auditors better grasp the intricacies of claim relationships and ensure accountability and transparency in decision-making.

A second key avenue is the extension of data and checks. Larger Medicare and Medicaid data sets, and data sets from other health care payment environments, could

be analysed in future studies. Other factors such as types of diagnoses, procedure services, and provider specialization could offer more context on payment patterns. Longitudinal analysis may also explore changes in provider behaviour over time and if there are any patterns of recurring irregularities over time. Validation through expert review and administrative audit results may enhance the relevance of the analytical results and help to create more robust processes for claims validation anomaly detection and improper payment risk evaluation.

CONCLUSION

Fundamental Finding: The research has been conducted using the Medicare claims data, exploring claims validation anomaly detection and improper payment risk assessment using an exploratory data analysis and explainable artificial intelligence approach. The analysis examined provider fraud indicators, distributions of reimbursements, number of claims by provider and number of claims per provider, provider-level distributions of provider characteristics and number of claims by provider, and beneficiary characteristics. The results showed that certain providers have a high number of claims and reimbursements in months where they had a higher number of fraud indicators and that a large portion of providers with a higher number of fraud indicators are engaged in unusual billing activities. Data from the correlation analysis revealed significant relationships between reimbursement measures, claims activity, and the available fraud indicators, and comparatively weak relationships between the beneficiary demographic characteristics and any other indicators. A second area of integrated anomaly analysis revealed provider profiles that were significantly different from the overall trend in healthcare payment patterns. **Implication:** It proves that visual exploration of claims data in healthcare is not only transparent, but can also help identify billing patterns, billing irregularities, and provider risk characteristics that are interpretable in terms of the healthcare payment landscape while fostering responsible interpretation and informed healthcare payment oversight. **Limitation:** While these observations are not evidence of fraud or inappropriate payments, they serve as helpful clues in conducting structured administrative review. **Future Research:** Future research should validate the identified billing anomalies and provider risk indicators using confirmed fraud cases and administrative investigation outcomes to assess their accuracy in detecting improper payments. Further studies should also integrate additional claims data, provider characteristics, and beneficiary information to improve the reliability and generalizability of explainable artificial intelligence models. In addition, future research should evaluate the effectiveness of these models in supporting timely administrative reviews, reducing false-positive alerts, and strengthening transparency and accountability in Medicare and Medicaid payment oversight.

REFERENCES

- [1] Centers for Medicare & Medicaid Services, “2023 Medicare Fee-for-Service Supplemental Improper Payment Data,” Dec. 7, 2023. [Online]. Available: <https://www.cms.gov/data-research/monitoring-programs/improper-payment-measurement-programs/comprehensive-error-rate-testing-cert/cert-reports/2023-medicare-fee-service-supplemental-improper-payment-data>.
- [2] R. Muhammad et al., “Fraud detection and explanation in medical claims using GNN architectures,” *Scientific Reports*, vol. 15, Art. no. 41734, Nov. 2025, doi: 10.1038/s41598-025-22910-6.
- [3] J. Kaur, G. Chawla, and A. Kumar, “Secure and explainable fraud detection in healthcare claims using blockchain-based machine learning,” *Scientific Reports*, 2026, doi: 10.1038/s41598-026-60701-9.
- [4] G. Adepu, “AI-driven healthcare payment systems using intelligent claims validation and fraud detection mechanisms,” *International Journal of Artificial Intelligence Research and Development*, vol. 2, no. 2, pp. 259–277, 2024, doi: 10.34218/IJAIRD_02_02_022.
- [5] P. P. Saha, R. Paul, M. R. K. Khan, N. A. S. Siddique, and B. D. Sarker, “AI-driven modernization of Medicare and Medicaid enterprise systems: Interoperability, claims analytics, and fraud detection frameworks,” *Journal of Intelligent Decision Making and Information Science*, vol. 3, 2026, doi: 10.59543/jidmis.v3.1223.
- [6] V. Kilanko, “The transformative potential of artificial intelligence in medical billing: A global perspective,” *International Journal of Scientific Advances*, vol. 4, no. 3, pp. 345–353, 2023. [Online]. Available: <https://www.ijscia.com/wp-content/uploads/2023/05/Volume4-Issue3-May-Jun-No.438-345-353.pdf>.
- [7] M. Hassan and M. Alam, “Automating healthcare claims processing with supervised and unsupervised AI models,” *Journal of Applied Big Data Analytics, Decision-Making, and Predictive Modelling Systems*, vol. 9, no. 2, pp. 1–11, 2025. [Online]. Available: <https://polarpublications.com/index.php/IABADP/article/download/2025-02-04/18>.
- [8] M. A. Sayem, N. Taslima, G. S. Sidhu, and J. W. Ferry, “A quantitative analysis of healthcare fraud and utilization of AI for mitigation,” *International Journal of Business and Management Sciences*, vol. 4, no. 7, pp. 13–36, 2024, doi: 10.55640/ijbms-04-07-03.
- [9] N. Kumaraswamy, M. K. Markey, T. Ekin, J. C. Barner, and K. Rascati, “Healthcare fraud data mining methods: A look back and look ahead,” *Perspectives in Health Information Management*, vol. 19, no. 1, article 1i, 2022. [Online]. Available: <https://pmc.ncbi.nlm.nih.gov/articles/PMC9013219/>
- [10] M. A. Nasir, N. Sultana, and M. A. Hasan, “AI-driven anomaly detection in U.S. government healthcare payment systems: Identifying improper disbursements and beneficiary fraud in federal public welfare programs,” *International Journal of Advances in Signal and Image Sciences*, vol. 11, no. 3s, pp. 176–192, 2025, doi: 10.29284/dzc7ah61.
- [11] S. K. Puli, “A hybrid LLM-graph architecture for laboratory billing discrepancy and overpayment risk detection,” *International Journal of Advanced Engineering Science and Information Technology*, vol. 8, no. 1, 2025, doi: 10.15662/IJAESIT.2025.0801002.
- [12] V. J. Patibandla, “Context-aware anomaly detection in healthcare claims using multi-stage decision pipelines,” *Power System Protection and Control*, vol. 54, no. 1, pp. 464–486, 2026, doi: 10.46121/pspc.54.1.30.

- [13] J. Kemp, Unsupervised Learning for Anomaly Detection in Australian Medical Payment Data. Ph.D. dissertation, University of New South Wales, Sydney, Australia, 2023.
- [14] R. Sugumar, "Explainable AI-driven secure multi-modal analytics for financial fraud detection and cyber-enabled pharmaceutical network analysis," *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, vol. 8, no. 6, pp. 13239–13249, 2025.
- [15] N. Parameshwarappa, N. R. Mudiya, S. R. Polu, M. Alla, and P. Koshiya, *Data-Driven Decisions*. USA: Cari Journals USA LLC, 2025.
- [16] D. Goswami, "Advancing threat detection through artificial intelligence and machine learning enhanced cybersecurity audits," *American Journal of Scholarly Research and Innovation*, vol. 4, no. 1, pp. 428–457, 2025.
- [17] A. W. Kräuterwald, "Cloud-Native AI and ML Solutions for Financial Risk Optimization in Healthcare ERP Environments," *International Journal of Computer Technology and Electronics Communication*, vol. 5, no. 3, pp. 5132–5139, 2022.
- [18] Zhou, "HEALTHCARE PROVIDER FRAUD DETECTION ANALYSIS," *Mendeley Data*, vol. 1, Apr. 2024. [Online].. doi: 10.17632/552r52kmg1.1
<https://data.mendeley.com/datasets/552r52kmg1>

Md Shakil Islam

Masters of Science in Business Analytics

Trine University, USA

Email: shakil23pha@gmail.com

Nishat Margia Islam

Master of Science in Information Technology

Washington University of Science & Technology, USA

Email: nishatmargiaislam01@gmail.com
