Evolving Systems (2025) 16:72
https://doi.org/10.1007/s12530-025-09698-6

ORIGINAL PAPER

Healthcare fraud detection using adaptive learning and deep learning techniques

Irum Matloob[1] · Shoab Khan[1,2] · Rukaiya Rukaiya[1,3] · Hessa Alfrahi[1,4] · Javed Ali Khan[1,5]

Received: 23 November 2024 / Accepted: 9 May 2025

Abstract

The healthcare industry faces huge losses due to the mismanagement of insurance transactions. Due to the development of public and private healthcare programs, many citizens receive better medical care benefits. Still, there is a need for financial transparency in these healthcare transactions, which has become a challenge. To ensure the delivery of more effective and higher-quality healthcare services, introducing healthcare fraudulent transactions prevention and detection tools in hospitals is necessary. In this paper, we propose how to inculcate a healthcare transaction monitoring system within an enterprise or organisation. Using machine and deep learning techniques, this research proposes a novel framework for analyzing health insurance data. Due to the complexity of medical information, detecting fraudulent transactions in the industry requires effort. Typically, patients, services, and providers (doctors, hospitals, pharmacies) are the main key elements of the healthcare ecosystem. As fraudsters continue to evolve their methods of conducting fraudulent transactions over time, an evolving fraud detection framework needs to be developed. Therefore, we proposed a framework that can identify fraud at the actor-level and further analyze the identified element (doctor, patient, and services) using an Anomaly transformer to evaluate the behavior of that particular identified element. Actor-level frauds are detected, 50% are at the patient level, 12% are at the service versus doctor level, 13% are at the service versus patient level, and 25% are at the physician level. Further, sequences of these elements are analyzed by the Anomaly transformer. All patient sequences' anomaly scores are generated using a data-driven threshold, and fraudulent sequences are identified. Results of the Speciality-based Rule engine and the Anomaly transformers are compared to identify the anomaly finally. Once the frauds are identified, the proposed architecture enables the management to take disciplinary action against each involved element. The Accuracy of the proposed framework is 97%, The experimental results are validated using the insurance data of local hospital employees, and the domain expert has validated the detected fraud cases.

Keywords Anomaly detection · Fraud detection · Healthcare · Insurance management · Sequence mining · Anomaly score · Anomaly rank

1 Introduction

The traditional insurance industry processes are based on predefined rules defined by experts and manual audits. These manual processes can not detect anomalies in the data automatically. The manual processing of insurance claims is time-consuming and degrades efficiency (Reis et al. 2022). The existing insurance management systems are based on predefined rules (Eling et al. 2022). The predefined rules limit the system's accuracy, as such systems cannot detect the new type of fraud. Whenever a new kind of fraud emerges, the rule engine is updated manually for the fraud. The existing insurance management systems are not scalable as they are based on manual processes (Baran 1987). The

✉ Irum Matloob
irum.matloob@fjwu.edu.pk

1 Fatima Jinnah Women University, Rawalpindi, Pakistan

2 National university of science and technology (NUST), Islamabad, Pakistan

3 Sir Syed University of Engineering and Technology, Karachi, Pakistan

4 Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

5 Department of Computer Science, University of Hertfordshire, Hertfordshire, UK

Published online: 05 June 2025

false positive rates of these systems are very high, as these are based on predefined rules. There is a need to reduce the false positives in such systems. To mitigate these issues, business intelligence using machine learning algorithms is needed to enhance the performance of the insurance processing systems (Vinora et al. 2023).

Healthcare services are business processes or entities that include prescription medications, diagnostic tests, and other treatments for patients (Bieberstein 2006). Based on past performance, business intelligence helps in decision-making in the business world. Most countries are introducing medical support programs to help their populations. For example, A healthcare practitioner was identified in 2018, who was charged with Medicaid for dollar 25 million in fraudulent claims, some of which included treatments that were never provided. The provider submitted bills for needless treatments while falsifying records (Palmer and Carter 2021). These medical assistance programs offer relief to their citizens. The primary anomaly in healthcare transactions and an obstacle to optimizing medical benefits is healthcare fraud (Wells 2019). It is an umbrella concept for three related ideas: Fraud, Abuse, Waste, and the intentional obtaining of illicit advantages. To increase a hospital's revenue, a doctor may prescribe pointless laboratory tests and medications; this is an example of waste. Likewise, a pharmacist who bills an insurance company and a patient for the same prescription is committing fraud. Suppose the pharmacist receives a prescription for a particular brand. In that case, the pharmacist abused his position. The patient actually receives a cheaper brand-name drug, and the insurer covers the cost of expensive brand-name drugs. Many of these dishonest acts count as healthcare fraud.

Healthcare fraud is a crime that affects many people and results in significant financial burdens for individuals and governments (Jr and Tobin 2020). It is necessary to detect healthcare fraud to reduce costs and improve the efficiency of healthcare services and insurance management systems. Many systems, namely Epic systems (Corporation 2023b), Cerner (Corporation 2023a), CommonWell Health Alliance (Alliance 2023), MEDITECH (MEDITECH 2023), etc, are proposed and implemented to improve the quality of healthcare services. According to recent studies (Bara et al. 2009; Ramalingam et al. 2024; Ivan 2014), software engineering methodologies and frameworks based on business intelligence using data analysis and machine learning techniques are now being adapted to solve all these healthcare problems efficiently. There is a need to introduce a methodology that can reduce monetary losses in the healthcare sector and improve the performance of insurance systems.

1.1 Research contributions

The following are the research contributions of our study:

- We propose a framework that uses an association rule engine and an Anomaly transformer to detect fraudulent transactions.
- The system can identify actor-level frauds using an adaptive learning approach. The Rule engine's rules can be updated and refined based on the new data and changes in the environment.
- We introduce the architecture for incorporating fraud detection and identification methodology in the insurance claim processing system.

2 Literature survey

A detailed study of the current concepts, methods, and approaches is mandatory to fully understand the benefits of integrating fraud detection in healthcare insurance systems.

2.1 Outlier detection methods

It is important to understand outlier detection methods in the context of fraud detection before proceeding with a formal literature review. There are two classes of outlier identification techniques. The first class of these algorithms finds anomalies in individual data points. In contrast, the second class of these algorithms builds the model while analyzing the data as a sequence. Most algorithms used in *beymani* (a collection of Hadoop, Spark, and Storm-based tools) fall into the first group of outlier algorithms. However, the real-time fraud detection algorithms must produce a model that can work in real-time (Gupta et al. 2014).

2.2 Fraud detection in healthcare using machine learning algorithms

Many research studies have recently been conducted to identify fraudulent activities in healthcare systems, as there is an urgent need to monitor the clinical care and financial utilization processes in the healthcare ecosystem. In healthcare, fraud can occur in three different ways. The first level of fraud detection includes hospital procedures (services), the second level includes disease diagnostics, and the third level includes system actors. Recent studies show that using applications based on statistical and machine learning techniques to study healthcare systems is increasing. In Yang and

Hwang (2006a), a strategy for automatically creating fraud detection models based on clinical pathways was presented. This data analysis was performed for Taiwan's National Health Insurance (BNHI). The proposed algorithm was able to detect fraudulent acts with 69% accuracy, but was unable to detect drug overdoses. Another model examined in Liu et al. (2016) was based on graph theory, designed to identify cases of waste and fraud in medical record entries. Three entities, a doctor, a patient, and a pharmacy, were used to generate a graph showing drug relationships. The same paper also included the study of a reference network instance where nodes were considered providers. The number of referrals between two nodes is displayed on the edges. Heterogeneous graphs can be used to understand the intricate connections between nodes better. Such complex relationship-based graphs are capable of detecting and helping to resolve millions of anomaly situations. The study cited in Musal (2010) uses clustering methods for geographic analysis to identify fraud. This investigation looked for cases of fraud by Medicare infusion treatment providers. Key clinical procedures are evaluated in Huang et al. (2012) for performance improvement. Patient care diaries are created to examine patterns in patient care and therapy. A density-based clustering method is then used to build anomaly detection models based on these patterns. The disease-based outliers were explored in Verma et al. (2017) to identify fraudulent activities, applying statistical rules to detect the disease-based and period-based outliers. All outliers were considered fraud. Healthcare projects often consider clinical processes for a specific disease and apply prior knowledge to unsupervised models (Okita et al. 2009; Van de Klundert et al. 2010). Authors in Peng et al. (2018), Anbarasi and Dhivya (2017) have developed frameworks to detect fraudulent activities by focusing on the correlation of diseases, drugs, and patients. Weights were assigned to the correlated data, and the frauds were detected based on these weights. However, a lot of research uses graph theory to describe different entities in healthcare systems, i.e., diseases, patients, and medicines. A correlation was found between the candidate set (extracted information). The reference set (actual knowledge). Most of this research was supported by previous information about the drugs used to treat various diseases.

2.2.1 Actor-level fraud detection

In addition to the research based on different health system entities, many studies have focused on fraud detection at the actor-level. It is clear that provider-level fraud, as opposed to patient-level fraud, has a greater negative impact on the healthcare system (Savino and Turvey 2018). In Ekin et al. (2019), unsupervised Bayesian hierarchical methods were used to detect fraud in health insurance claims, or claims that provide details about patients, physicians, and costs. Bayesian hierarchical methods can detect fraud and anomalies in medical bills. The authors of the study (Zafari and Ekin 2019) examined providers' prescribing patterns. This research used topic modelling to identify irrelevant or additional prescription patterns that resulted in unnecessary medications being prescribed. In Kose et al. (2015), a machine learning approach with hierarchical processing on weighted data of actors is used. These weights are assigned to actors without considering the actor's roles as clients or providers. Groups were formed using expectation maximization clustering techniques. In Cui et al. (2016), a logical treatment model is proposed based on the graph and frequent pattern mining approach. The same study also examined the doctors' reliability in considering the prescription copies. This measure can be critical in detecting fraud at the provider level. Although fraud is a collective act of many actors, most studies do not consider all actors in the healthcare system and analysis based on the relationships between these actors are often overlooked.

According to Itri et al. (2019), the random forest method outperforms all others with a detection rate of 23.8%. In Li et al. (2008), Joudaki et al. (2015), statistical data is used in conjunction with mining techniques, which can help users discover and analyze hidden historical data. Ortega developed a system that can identify 75 scams per month, which is not a very good Scam identification rate, as mentioned in Ortega et al. (2006). A system was developed in Sowah et al. (2019) using multi-layer perception neural networks for the Chilean private health insurance company. The accuracy of the model was 87.91%. This model is based on genetic support vector machines, which could detect irregularities and fraud in health insurance claims. Another method examined in Liu and Vasarhelyi (2013) considered location-based clustering for Medicaid providers and clients and was able to detect fake claims. In Yang and Hwang (2006b), an adjustable approach to automatic fraud detection in clinical operations was proposed through this framework. A graph mining technique was used to separate the distinguishing features from the expense and other features in the treatment sequence data of a gynaecology department. The model needed to be modified for the cost-specific site policy. In Thornton et al. (2014), a system is proposed for detecting fraud in Medicaid insurance claims data through unsupervised learning. Another study (Thornton et al. 2013) examined multidimensional methods to identify fake claims in Medicaid data. It is important to note that recent studies have leveraged Public Use Files (PUF) data from CMS to identify fraud by using data mining techniques used in Feldman and Chawla (2015), Herland et al. (2017), Bauder

et al. (2016), Bauder and Khoshgoftaar (2016b), Bauder and Khoshgoftaar (2016a), Bauder and Khoshgoftaar (2018), Chandola et al. (2013). Most of these studies used statistical methods to create the decision criteria and focused on "Part B" of the PUF data. K-means clustering on time series-based insurance claim data was used to find outliers and anomalies. To extract the critical patterns, fuzzy and Neuro-fuzzy analysis were used in certain studies (Gath and Geva 1989; Lenard and Alam 2005; Köppen et al. 2009).

Similarly, adjacency graphs were also used to separate normal and abnormal behaviour. In Liu et al. (2020), a new LSTM-based method proposal is presented. Another model was developed to predict false claims in automobile insurance systems (Kowshalya and Nandhini 2018). The model examined the J48, Random Forest and Naive Bayes algorithms. A second two-stage fraud detection mechanism was proposed in Subudhi and Panigrahi (2017). Fuzzy C-means clustering based on genetic algorithms was used to identify the fraudulent transactions. The second stage involves further verification of identified anomalous transactions using supervised Decision Tree (DT), Support Vector Machine (SVM), Group Method of Data Handling (GMDH), and Multi-Layer Perception (MLP) learners. In Seo and Mendelevitch (2017), a similar graph and ranking algorithm approach is used to detect vendor-level fraud. This study first created a chart representing medical prescriptions and then used the page rank method to find abnormalities at the second level. The mining technique was used to create rules for common things: association rule mining (Hristidis 2009). Other studies have explored this method to develop the rules and explore the domain. For example, in Altaf et al. (2017), Toti et al. (2016), Cai et al. (2017), two beneficial criteria, namely trust and support, were used to analyze the strength of association rules. Some features such as uniqueness, understandability, applicability and reliability were examined in Zeng et al. (2016) to evaluate created rules. The association rules were used by the developers of Ou-Yang et al. (2013) to determine the doctors' prescriptions. There are many other systems which are being introduced using deep learning approaches, as in Khan et al. (2024), the authors proposed a framework by combining CNN and transformers for detecting skin lesions. In Alrawili et al. (2025), the authors performed a detailed review of authentication issues in modern systems. In citearif2024towards, the authors presented electricity theft detection using deep learning techniques. In Si-Ahmed et al. (2024), a detailed survey is performed for intrusion detection in the IOMT environment. Authors in Khan et al. (2024) introduced embedding models for asymmetric relationships.

2.2.2 Fraud detection in other domains

Since fraud is widespread around the world, it makes sense to analyze both the healthcare systems literature and material from other areas. In Travaille et al. (2011); an in-depth study of fraud detection systems in various industries was conducted. The detection of fraudulent actions in the e-commerce sector is covered in Carta et al. (2019). The regulatory multiple consensus model used in the proposed method was validated on a real dataset that exhibited large imbalances. Compared to other state-of-the-art models, the validation results showed that the ensemble model performed at the highest level. It is observed that the research focus was mainly on detecting frauds and anomalies in the financial sector. Few have focused only on the connectivity details of the actors, i.e., telecommunication industry. Hence, there is a scope to focus on actors' association rather than financial analysis. It was also observed that none of the systems were able to detect all types of fraud at the actor-level.

2.3 Comparison to the existing systems in literature

The proposed framework integrates the idea of actor-level fraud introduced in Matloob et al. (2020), which was previously explored using the sequence rule engine proposed in Matloob et al. (2020). The identified fraud validity will be strengthened if we integrate these two concepts and finally introduce an adaptive learning-based fraud detection framework. As per the literature review, we have identified many systems based on the knowledge base of clinical processes. Fraud detection is performed mainly by identifying payment-related fraud. Fraud detection systems focus on the correlation between disease, patient, and medicine. There is a need for a system to identify fraud within healthcare transactions. Actor-level fraud detection is important to identify the main culprit within healthcare transactions. Our proposed methodology can identify doctor, patient and service-related frauds.

Secondly, in the literature, techniques are applied to payment procedures. Anomaly detection is performed to identify anomalies in a sequence of the same speciality. Payment and time lags are used to detect fraud. There is a need to propose a system which can analyse sequences of service availing and providing patterns for all specialities. Therefore, there is a need to incorporate a fraud detection system within the insurance processing system. There is a need for architecture on which we can implement the proposed methodology. We have proposed an architecture for incorporating

Table 1 Focusing key research papers on healthcare insurance predictability and fraud detection

Author(s)	Methodology	Description
Kaushik et al. (2022)	Artificial neural network	Accuracy is 92.72% and dynamic health parameters are not considered
Vuddanti et al. (2024)	Regression, Gradient Boosting is applied	Accuracy is 94% but real-time adaptability is not achieved
Jyothsna et al. (2022)	XGBoost and Telegram chatbot	Accuracy is 87%, but deep learning models are not applied
Fursov et al. (2022)	Sequence analysis using embeddings, Deep Learning	ROC AUC is 0.873 for fraud detection but no description about interpretability
Mavundla et al. (2024)	Random Forest, KNN, XGBoost	Random Forest achieved 99% accuracy, but regulatory and economic factors are not considered
Zhang et al. (2022)	Blockchain, Deep Learning (BERT-LE)	Improved fraud detection based on predefined rules

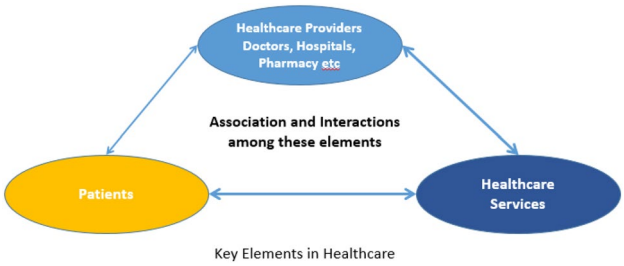

Fig. 1 Healthcare key elements

a fraud detection system within the insurance processing system.

In this section, we discussed all existing techniques for healthcare fraud detection in the above paragraphs. We have discussed the features of the insurance systems, which are addressed in most of the research in Table 1. A framework is needed to incorporate healthcare fraud detection in insurance processing systems. There is no such insurance system in which a fraud detection feature is included. All the above-mentioned systems detect fraud based on payments or identify one type of actor-related fraud. The hour must consist of a fraud detection system in the insurance claim management system. By doing this, we can identify the fraud at the right time, and this could improve the overall performance of the insurance processing systems.

3 Proposed framework

This section describes a novel framework for integrating fraud detection in healthcare insurance systems. Firstly, we discuss a framework for a fraud detection system, and after that, we discuss how we can include a fraud detection system within the insurance claim management system. The proposed architecture is provided at the end of this section.

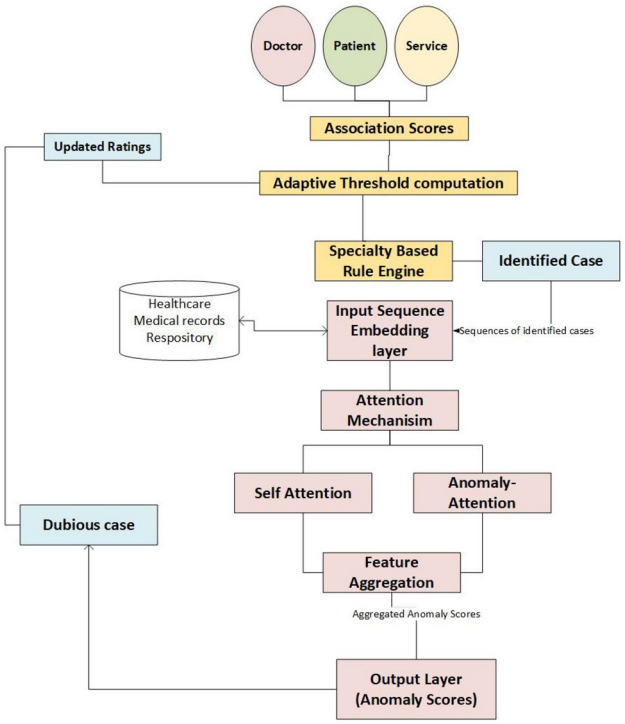

Fig. 2 Overall workflow of proposed framework

The three main components of the proposed framework are patients, providers (doctors, pharmacies, and hospitals), and connected services. These are interacting elements within the healthcare ecosystem, as shown in Fig. 1. Due to the complex relationships among these three elements, analyzing healthcare data is difficult.

In this framework, we first identify anomalous cases at the actor-level and then create time series traces of patients to examine a single element's behavioral patterns. The system consists of two cascaded modules that detect fraudulent and suspicious transactions, as shown in Fig. 2.

The healthcare fraud detection system first implements a rule engine, the Association rule engine, and then an

Table 2 Abbreviations for the used terms

Abbreviation	Description
Y_{ij}	Doctor (Association score)
D_j	Patients examined by doctor
P_i	No of patients
S_{ji}	Patient (Association score)
p_v	Total number of visits of patient
U_{li}	Service with Patients (Association score)
g_{li}	No of transaction when doctor D_j suggested service m_l to patient P_1
m_p	No of transactions when all doctors wrote service m_l prescribed to Patient P_2 (for all services)
$F\_\{li\}$	Service with Doctor (Association score)
T_{lj}	No of transactions when doctor D_j prescribed service S_l
p	No of transactions when all doctors prescribed service S_l

Anomaly transformer is implemented to identify anomalous sequences. The association rule engine implements the following three stages for identifying fraudulent actions: first, it computes association scores; then, the association rule-based engine implementation; and then, the similarity check function.

The technique consists of three cascaded phases. Healthcare data is used to identify fraud; such records can be used to identify outliers. In the first phase, suspicious or anomalous cases are identified. In the second phase, the rule engine is used to thoroughly investigate the cases found in the previous phase. Each current transaction is compared to the generated rules in the third phase. This computes the association among the doctors, the patients, and the services. The rating score for the specific element is decreased each time a fraud instance is found.

The three components' interactions are thoroughly examined and computed using the association scores, which must be determined between each element. The association scores are calculated based on the frequency of visits or prescriptions. Suppose a patient regularly goes for a particular service (like X-rays or ECGs). In that case, he or she may receive numerous ECG prescriptions from the same doctor, which is an anomaly. Based on how frequently patients visit doctors and other providers of services, we calculate association ratings. The goal is to provide the rule engine only with anomalous patient records. The notation used is listed in Table 2.

- Doctor (Association score) Y_{ij} is calculated using Eq. 1.

$$Y_{ij} = (P_i / \sum_{j=1}^{n} D_j) \tag{1}$$

  n is the total number of transactions of doctor D_j.
- Patient (Association score) m_{ji} is computed as number of times doctor D_j examined patient P_i and p_v representing the total number of patients' visits P_i (for all patients) in Eq. 2.

$$S_{ji} = (m_{ji} / \sum_{i=1}^{v} p_i) \tag{2}$$

- Service with Patients (Association score) is computed using Eq. 3.

$$U_{li} = (g_{li} / \sum_{l=1}^{p} m_l) \tag{3}$$

- Service with Doctor (Association score) is computed using Eq. 4.

$$F_{li} = (T_{li} / \sum_{l=1}^{p} m_l) \tag{4}$$

The range of association scores is between 0 and 1. The purpose of finding association scores is to filter out those records with greater frequency and forward only these records to the rule engine for evaluation, which is proposed in Matloob et al. (2020).

The anomalous cases are identified based on these checks. For each framework component, the rating score is initially set to 100. Following the first phase, the rating score is updated based on the occurrence of identified cases. The rating of that specific element is decreased each time an anomalous case is discovered. In the second step, anomalous cases are examined.

The second stage of the proposed framework generates rules for each speciality. It has already been mentioned that the original data from the local international hospital is used to validate the proposed framework. The 32 specialisations that this hospital offers. The rule engine is generated based on the sequence of steps. The most important thing is to de-identify patient records. Each patient, doctor, and Service is assigned a unique Patient number $patient_n$, doctor

ID $doctor_n$, and service identifier $service_n$. Patient records are grouped based on the services used by the specialty_id. G-means clustering is used to identify clusters. In each cluster, we have availed services from the speciality. Clusters are analyzed further to compute Support and confidence values using Eqs. 5 and Eq. 6. S_h is the service whose support is being computed where h is representing several services. $Count(S_h)$ is the number of occurrences of a particular service within the cluster and $cluster_n$ is the total number of services in clusters. Where the total number of components in a cluster is $cluster_n$.

$$Support(S_{hn}) = Count(S_h)/cluster_n \tag{5}$$

$$Confidence(S_h \cap D_j) = Support(S_h \cap D_j)/Support(S_{hn}) \tag{6}$$

Within clusters, we calculated a confidence value for each service. For all cluster members, we apply a data-driven threshold to the confidence values, and those whose confidence values lie on the boundaries are labelled as anomalous. The second phase illustrates how clusters are processed to produce rules. To create rules, the support count for each specialty D_j across all clusters and the support count for each service S_h for that specialty D_j are determined.

Finally, confidence values are computed using these support counts. The rules are created and stored in a database for the third phase based on the calculated confidence levels. Calculating the similarity between the current transaction (c) and the created rule (R) is done using the similarity function using Eqs. 7 and 8, respectively. Where, a represents the similarity bit and b represents the similarity function H. For rule R, the service i received from speciality j is known as $Service_{ji}$. The threshold for services i received from speciality j is T.

$$Rule\ R = Service_{ji}\ with\ C_{ji} > T_{ji} \tag{7}$$

$$Similarity\ function\ H = R \cap c \tag{8}$$

If the size c of the input transactions after similarity calculation is equal to the size of the similarity function H, the similarity bit is set to 1; otherwise, it is set to 0.

Transactional data is obtained from each of the three main parts of the hospital servers. Every patient, every service, and every provider has its storage. For each pair, association scores are calculated, including service scores for the doctor, service scores for the patient, patient ratings for the doctor, and doctor scores for the patient. After computing the association scores and applying the thresholds, we obtain a set of identified cases. Two incidents show that certain transactions are anomalous. Any patient, provider, or service whose transactions are deemed suspicious will have their rating reduced. The rule engine receives these cases as an input. The implicated element's rating score will be reduced if fraud is discovered after subsequent transaction analysis by the Rule engine; otherwise, the rating score will remain the same. For each specialty_ID, a set of rules are essentially produced each time a patient enters the hospital to utilize a specific set of services. The framework decides which specialty_ ID the patient sees first. Then it analyses the patient per the rules already computed for each speciality_ID.

Therefore, we examined this transactional data by considering three components of the suggested framework and found varying numbers of healthcare frauds. Each specialty's_ID (specializations like cardiology, urology, etc.) has a set of services with confidence levels that define its rules. The rule engine was created using data from five years of medical transactions. Hospital analysts can not analyze millions of records, but with the help of the proposed framework, he/she can investigate 5% of the cases.

Once the association rule engine has identified suspicious cases, the sequence rule engine forwards these cases for detailed analysis. Using the Sequence Rule Engine, we can evaluate the patient sequences related to the suspicious element. The sequence database is generated by converting healthcare transactions into time series sequences. Then, the Anomaly transformer is applied. The anomalies detected by the anomaly transformer validate the anomalous cases identified by the Rule engine. We cannot detect anomalies directly from the patient time series traces, so we independently determine the sequences of patient transactions for each speciality. The course of treatment of each patient for each speciality is documented.

Let S represent a group of services, T represent the date those services were used, and ε represent the set of all feasible service event identifiers. Service events are assumed to have a range of characteristics. An example of a clinical service event would include the date of the service, the speciality where the event took place, and the names of medical experts or doctors who prescribed the services.

A series of service events is used to illustrate a patient time series trace. Each service event has a multiple appearance limit and does not decrease over time. We take into account the patient information detail P, which includes the patient's MR_No P_m, service date S_d, and service event type S_t as described in Eq. 9.

$$\forall P = (P_m, S_d, S_t) \tag{9}$$

Clinical service type and service date are the two primary qualities we consider. Their respective functions are $\alpha_s \in \varepsilon \rightarrow$ S and $\alpha_t \in \varepsilon \rightarrow$ T. Therefore, e=$\{\alpha_s,\alpha_t\}$. Equations 10 and 11 define the patient sequence *epsilon* and patient time series trace γ, respectively.

$$\epsilon = \{e_1, e_2, e_3 \ldots\ldots e_n\} \tag{10}$$

$$\gamma = \{\epsilon_1, \epsilon_2, \epsilon_3 \ldots . \epsilon_n\} \tag{11}$$

Patient sequences are essential services that patients receive. A collection of all patient sequences across several disciplines generates a patient time series trace. If two events occur on the same date, they are arranged in the time series trace according to the transaction_id.

Let L be a speciality history and Sim(ϵ,p) be the similarity measure for any two sequences ϵ and p in L. The L can be partitioned into multiple specialities; in our case, there are 62 specialities φ_1,....,φ_{62}. Speciality sequence φ is described in Eq. 12.

$$\varphi_i = \{c_1, c_2, \ldots, c_n\}, \quad i = 1, 2, \ldots, n \tag{12}$$

Therefore, $\epsilon_i \in \varphi_i$ where i represents a number of specialities. There are several patients traces ϵ in the medical speciality φ. The α_a and α_t are the two components of each patient trace.

The Anomaly transformer finds dependencies in time-series data by using an attention technique. It distinguishes between typical patterns and anomalies, however, by concentrating on the degree to which one timestamp in the series affects another, in contrast to traditional Transformers. It makes use of both normal and anomalous attention. While anomaly attention finds odd, unexpected links in the data, normal attention concentrates on common patterns. This dual approach aids the model in learning both typical patterns and anomalies.

The anomaly transformer gives an anomaly score for every timestamp. This is accomplished by assessing the likelihood of each point relative to the others and computing a probability distribution over the series. A high anomaly score is given to timestamps where the attention deviates from predicted patterns after comparing the attention scores at each point. As a result, timestamps that are less likely to fit the typical data distribution are highlighted by the model.

The model additionally uses the patterns discovered from the attention scores to reconstruct the time series and forecast future points. When reconstructing the time series, the Anomaly transformer may assess how well each point fits anticipated patterns. A point is probably an anomaly if it doesn't match well during reconstruction, meaning the prediction and the actual data diverge significantly.

By comparing the consistency of the normal and anomaly attention ratings, the loss function of the Anomaly transformer incentivizes the model to differentiate between normal and anomalous data. The model can learn when attention patterns suggest normal behavior and when they signal abnormalities with the help of this loss function.

One of the anomaly transformer's benefits is its interpretability. By looking at the attention scores, it is possible to determine which timestamps are most important in detecting an abnormality. We have used different numbers of attention heads and variations in hidden dimensions to handle the model sensitivity. A custom attention mask is also used to emphasize the services and specialities, as depicted below.

$$\text{mask}[h,k] = \begin{cases} 0 & \text{if } h \text{ and } k \text{ are focused time steps} \\ -\infty & \text{otherwise} \end{cases}$$

Attention mechanism consists of three main components: Query Q, Key K and Value V. These components determine how much attention will be given to each sequence element.

Query Q is the feature that "queries" other sequence elements for attention. In your situation, the query vector would be a learnt representation of the service and its speciality if each sequence element matched a service rendered. This indicates to the model what data each component looks for from the others.

Keys K are characteristics of every element that "match" or answer the question. Each service-speciality pair would produce keys that other services or specialities might query for pertinent information if the attention mechanism concentrated on service and speciality features.

Each element's actual information in response to attention is stored in values V. Based on the keys and queries, the values obtained from services and specialities would include data the model deems significant.

$$Q_i = W_Q \cdot \begin{bmatrix} \text{Service}_i \\ \text{Specialty}_i \end{bmatrix}$$

$$K_i = W_K \cdot \begin{bmatrix} \text{Service}_i \\ \text{Specialty}_i \end{bmatrix}$$

$$V_i = W_V \cdot \begin{bmatrix} \text{Service}_i \\ \text{Specialty}_i \end{bmatrix}$$

$$\text{AnomalyScore}_t = \frac{1}{T} \sum_{j=1}^{T} D_{tj}$$

The Anomaly transformer is implemented to identify the anomalous transactions; it helps to capture time-based dependencies in the generated sequences. The length of input sequences is set to 30, and the model is configured accordingly, which enables the model to examine patterns within all transactions. The model outputs the anomaly scores for all transactions, and anomalous transactions are detected based on the anomaly score. This further validates the result of our methodology.

The rule engine further evaluates the detected anomalies. If the detected anomaly is actual, disciplinary action will be taken. If no rule is related to the generated anomaly, the rule engine is adaptively updated. The complete workflow is explained in Algorithm 1

Algorithm 1 Detailed Workflow of the Proposed Methodology

Input: Doctor, Patient, Service, UpdatedRatings **Output:** Anomaly Scores, Dubious Cases

Step 1: Compute Association Scores AssociationScores ← Compute Association Scores(Doctor, Patient, Service)
using equations 1,2,3,4
ThresholdedScores ← Apply Adaptive Threshold(AssociationScores)

Step 2: Apply Specialty-Based Rule Engine IdentifiedCases ← *set* **for** E **do**
a
chscore ∈ Thresholded Scores **if** *SpecialtyRuleEngine(score) == TRUE* **then**
IdentifiedCases.append(score)
using equations 5,6,7,8,.

Step 3: Anomaly Detection with Transformer Train AnomalyTransformer on Historical healthcare transactions
EmbeddedSequence(γ) ← Sequence Embedding (IdentifiedCases + historical medical record sequences)
Attention Output(δ) ← ApplyAttention (γ)
Self attention(α) ← Self Attention(δ) Anomaly Attention(ϵ) ← Anomaly Attention(*delta*)
Features (β)← FeatureAggregation(α, ϵ)
Anomaly Scores(λ) ← OutputLayer((β)

Step 4: Final Evaluation **for** $i \leftarrow 1$ **to** *len(*λ*)* **do**
if *λ[i] ¿ Threshold* **then**
Mark As Dubious(IdentifiedCases[i]) Update Ratings(IdentifiedCases[i])
if *AnomalyTransformer Detected(IdentifiedCases[i])* ***and*** *Rule Engine Flagged(IdentifiedCases[i])* **then**
Confirm Anomalous Case(IdentifiedCases[i])

Once healthcare frauds are detected, we can identify the suspicious doctors, patients, and services involved in the identified transaction. The insurance management system will be adapted to take disciplinary action against these elements and reduce their rating. This can improve the performance of the insurance management systems.

4 Results and discussion

4.1 Case study

The proposed framework is validated based on five years of transactional data on employee insurance claims from a local hospital [2013 to 2019]. The size of the transaction record is shown in Table 3. The attributes taken into account by the frameworks are listed.

Figure 3 shows the gender-based amount utilization and the anomaly in a particular lower abdominal test. Females are availing of this hospital's services more frequently than males.

Although women are more likely to undergo pelvic examinations, there are some cases in which men also undergo this examination. To identify which age group of employees or patients is availing services more, we have analyzed historical data and found that employees aged 21–35 years are availing more services, as depicted in Fig. 4.

Table 3 Attributes provided in patient's dataset

Name	Value
Service_IDs	1200
Physicians	486
Specialty_IDs	62
Patients medical transactions	440,000

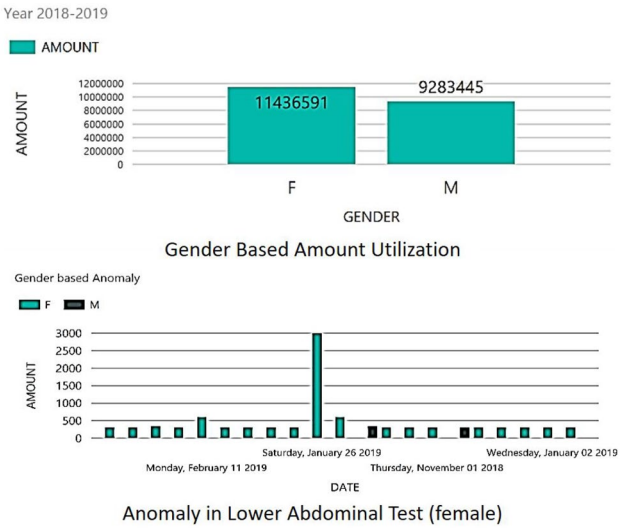

Fig. 3 Transactions of hospital employees based on gender

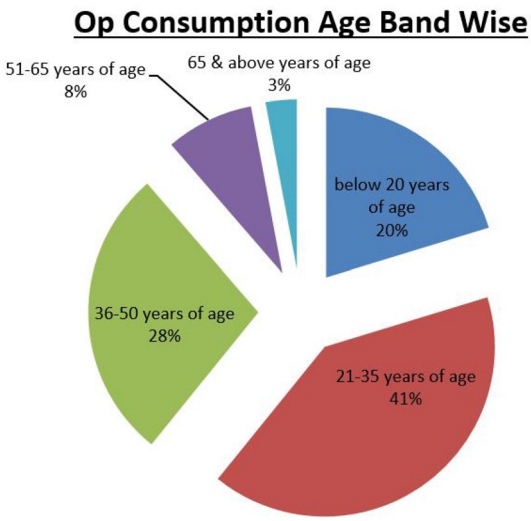

Fig. 4 Age-wise analysis of medical record

The hospital's major specialities generating more expenses are identified as depicted in Fig. 5.

4.2 Feature selection

Feature reduction is performed using the Recursive feature elimination method. Figure 6 depicts the computed scores for all features.

The data-driven threshold is computed to select the related features for initiating analysis.

The actor-level fraud detection model is used to analyze and find potential fraud cases in the dataset. Then, the Sequence rule engine further examines anomalous cases.

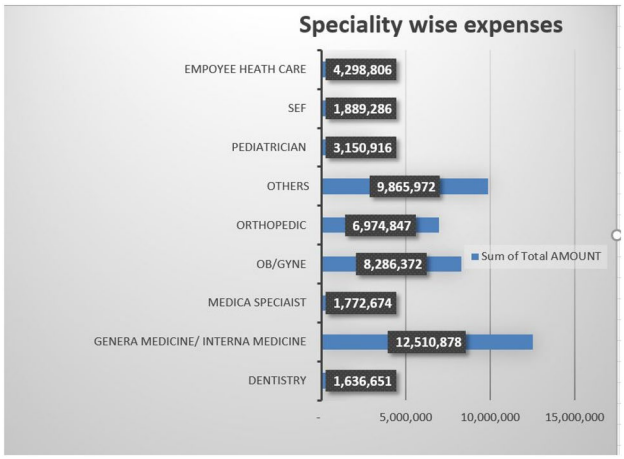

Fig. 5 Expenses of medical specialities

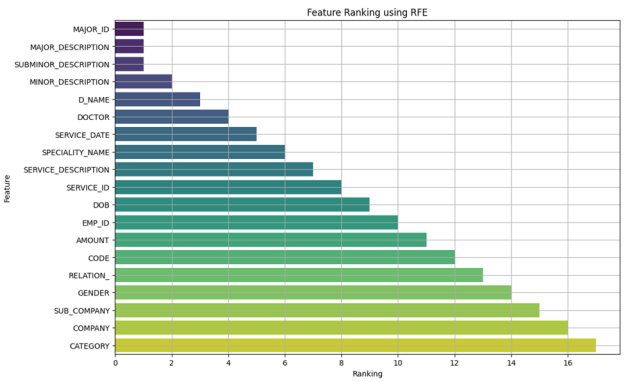

Fig. 6 Recursive feature elimination outcome

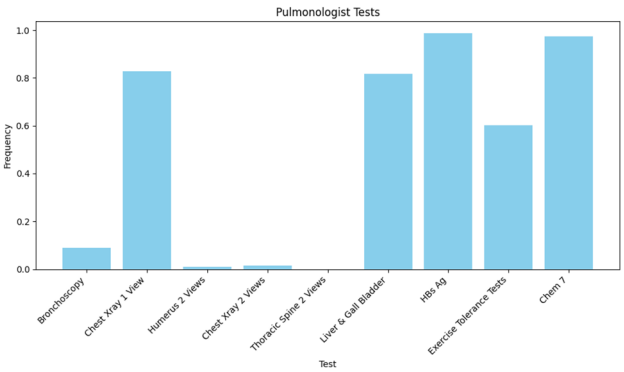

Fig. 7 Few patient services availed from pulmonologists and their confidence values

4.3 Healthcare fraud detection system

In the first phase, the association scores between each pair of elements are computed. The main task is to generate the

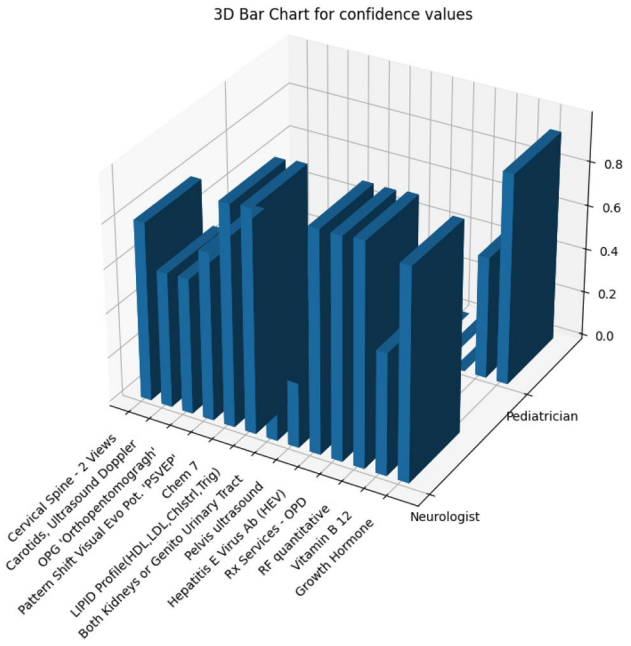

Fig. 8 3D chart for confidence values

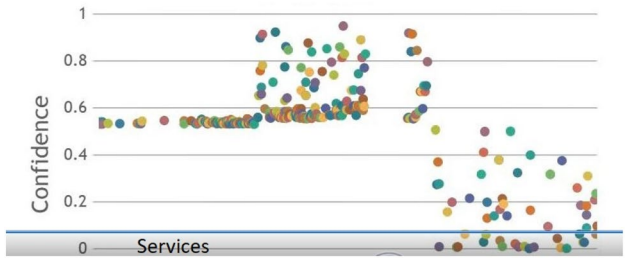

Fig. 9 Services availed from specialties and their confidence values

confidence value of each service for each specialty. Once confidence values are calculated for each service within each speciality, the data-driven threshold is computed. This threshold is also adapted as we have to recompute it once a fraud case is detected. Users can select the threshold based on their scenarios. The rule only includes *service_ids* whose confidence values are greater than 0.001. An example will help to understand the rule that the rule engine produced. Table 8 displays the services used from this speciality and provides confidence values for those services. The rule for this speciality is generated from this table. Any transaction in which the patient receives "Exercise Tolerance Tests" service from the Pulmonologist speciality. The similarity function first determines whether this service is specified in the rule for the speciality as listed in Fig. 7. Since 'Exercise Tolerance Tests' services cannot be provided in the field of Pulmonologists, this instance has been classified as an anomaly. Additionally, a transaction that involves the use of healthcare services from the considered specialty and whose confidence value is less than 0.001 is flagged as fraudulent and sent to the analyst dashboard for additional analysis. The rules are generated for all specialities using the historical transactional data. The confidence values of services the Paediatrician and Neurologist availed are depicted in Fig. 8. Figure 9 depicts confidence values of each service for each speciality, and in these figures, specialty_id and service_ID are used. On the x-axis, we have confidence values, and on the y-axis, we have services.

Figure 10 shows that only a few services have high confidence scores. High numbers show that this specialization performs these services more frequently. In contrast, low values show that this speciality performs these services less frequently.

After the evaluation from the association rule engine, the sequence rule further analyses all detected cases. The algorithm for the association rule engine is discussed in Matloob et al. (2020). However, we have not specified in previous research how to use results from association rules to detect fraud sequences.

After converting transactional data into a sequence database, we obtain patient sequences for every speciality. The sequences for the medical specialist subset are shown in Table 4.

The sequence database implements an Anomaly transformer and computes normal and anomalous sequences. Frequent sequences for *medical specialist* speciality as shown in Table 5.

The frequent sequences generated in *Pediatrician* Specialty are shown in Table 6.

In this methodology, we have generated the anomaly scores of each sequence within each speciality.

The knowledge base is generated based on each speciality's anomaly score sequences of services. All frequent and less frequent sequences used in this speciality over the previous five years were used to derive sequence rules using anomaly scores.

4.4 Comparison with state of the art techniques

We compared our current methodology with some related research studies, as listed in Table 7.

There are very few fraud cases in healthcare transactions, which means such datasets are imbalanced. When Machine learning techniques are applied to such imbalanced data, they produce biased results by predicting non-fraudulent transactions as fraud. We need to apply careful and regressive tuning to avoid over-fitting and under-fitting.

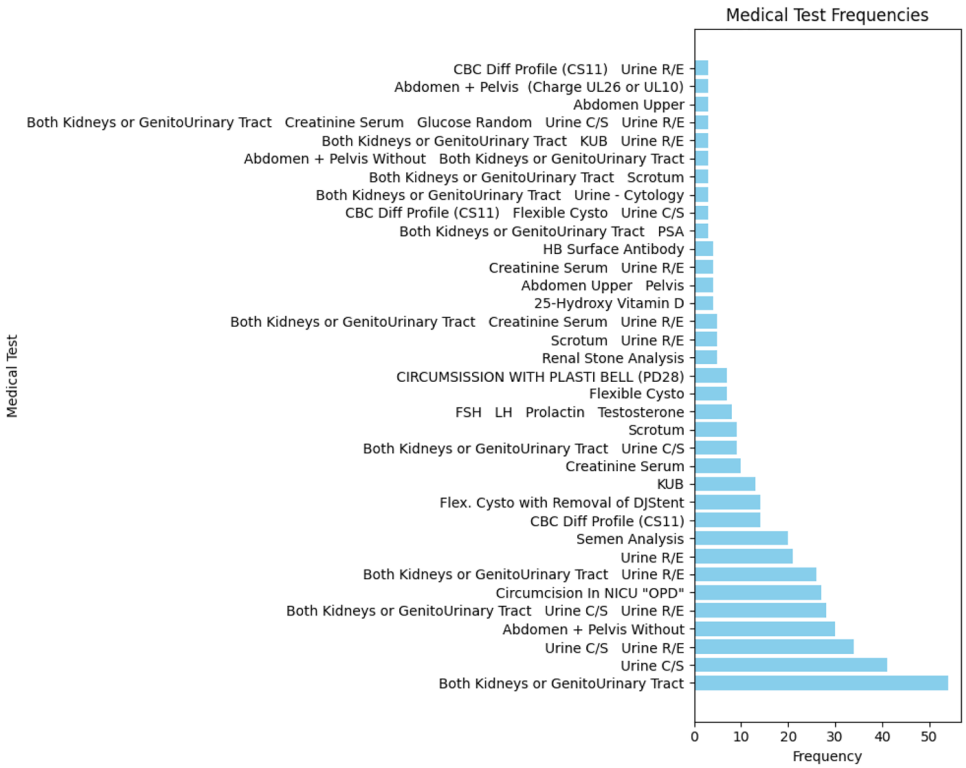

Fig. 10 Confidence values for specialities

Table 4 Subset of patient sequences of services availed in medical specialist

Sequence	Specialty ID	Specialty Name	MR_NO
1769 1756 3280 1600 1533 1594 1777 1351 1339 1878 13556 13556 13556 13556 13556 13556 13556 13556 13556 13556	29	Medical Specialist	11148
1583 1584 1504 5323 1594 1602 1603 1607 1584 1504 1602 1603 1607 1603 1607 1584 1504 1602 13556 13556 1969 1969 1602 1583 1584 1504 5323 1715 13556 13556 13556 13556 13556 13556 13556 1969 1504 1603 5323 13556 13556 13556 13556 8842	29	Medical Specialist	1115
1644 13556 13556 13556 13556 1827 1769 1762	29	Medical Specialist	11150
13556 1769	29	Medical Specialist	11151
4783 13556	29	Medical Specialist	11155
8815 13556 1969 3280 13556 13556	29	Medical Specialist	11164
3280 13556 13556 15852	29	Medical Specialist	111650
13556 13556 1969 4783	29	Medical Specialist	11201
13556 13556 1969 3500 8815 13556 13556 18245	29	Medical Specialist	112233
13,556 3280	29	Medical Specialist	11232

The proposed methodology can detect possible anomalous behaviors. Three primary levels of cascaded checks can be conducted:

1. The association rule engine detects Anomalous transactions of each element in the healthcare ecosystem.
2. Patients, doctors, and services that are detected as frauds by the association rule engine are further analyzed by the Anomaly transformer.

We can see from the Table 8 that each speciality has a rule, which depicts which services are permissible for this particular speciality. When the rule engine and Anomaly transformer identify any actor as a fraud, it will be forwarded to the management for disciplinary action.

Figure 11 lists a few instances of Fraud cases. All these transactions involve health services which are not permissible for the said speciality.

The Fig. 12 depicts the anomaly rank of specialties based on the anomalous transactions. The healthcare providers validate these anomalous transactions.

Table 5 Medical specialist frequent sequences

Sequence	Minimum support	Specialty ID	Specialty name
1909 1769	149	280	Medical Specialist
1909 1796 1594	37	280	Medical Specialist
1909 1769 1602	39	280	Medical Specialist
1909 1769 1909	33	280	Medical Specialist
1909 1769 7879	30	280	Medical Specialist
1909 1769 1756	31	280	Medical Specialist
1909 1769 1769	44	280	Medical Specialist
1909 1533	76	280	Medical Specialist
1909 1533 1769	35	280	Medical Specialist

Table 6 Pediatrician frequent sequences

Sequence	Minimum support	Specialty ID	Specialty name
8710 3956 1969	17	490	Pediatrician
8710 3956 3956	15	490	Pediatrician
1548	71	490	Pediatrician
1548 1552	27	490	Pediatrician
1548 1552 1769	16	490	Pediatrician
1548 1969	29	490	Pediatrician
1548 1604	16	490	Pediatrician
1548 1878	15	490	Pediatrician
1548 1769	42	490	Pediatrician

There is a dire need to discuss false positives within the predicted results to evaluate the model's performance. Our model has achieved good accuracy for all specialities, but we can see that the anomaly score is high for a few specialities. When the anomaly score is high, there are many false positives, making it difficult to identify true anomalies. Figure 13 depicts the rate of false positives. We have performed a thorough validation process to reduce the number of false positives from our proposed methodology and adjust the data-driven thresholds accordingly. By reducing the false positives from our model, we have increased the reliability of our methodology.

We have analysed the performance of the anomaly transformer. We have tried different learning rate values to improve the transformer's performance, as depicted in Fig. 14. Learning rate value 0.001 is more applicable in our case.

The Table 9, explains the performance evaluations of the proposed framework.

Figure 15 shows how accuracy improves over each epoch. If the training accuracy is high but the validation accuracy is low, then the model might memorize the training data, but our model generalizes well because there is a small and consistent gap between the training accuracy and validation accuracy lines. As mentioned, our dataset is unlabelled, but we have validated our anomalous cases from the domain experts(a Team of doctors). We have marked the cases they identified as actual anomalies. Based on this validation, we have computed the accuracy of our methodology.

Figure 16 depicts precision, Recall, and F1 Score, and as we know, these are critical for evaluating the anomaly detection model, especially with class imbalance. The precision measures the proportion of detected anomalies that are actually anomalous. A drop in precision, while an increase in recall, may indicate many false positives. The recall tells how many actual anomalies the model correctly identifies. The F1 Score helps to evaluate the model's robustness under an imbalanced dataset. Actor-level frauds are detected, 50% are at the patient level, 13% are at the service versus patient level, 12% at the service versus doctor level, and 25% are at the physician level.

Table 7 Comparison with existing methodologies

Researches	Data driven knowledge base	Specialty specific	Unsupervised approach	Fraud type	Payment based analysis	Validation
Massi, M. C., Ieva, F. & Lettieri, E. (2020) Y. Gao, C. Sun, et al (2018)	NO	Hospital Discharge Charts based behavior analysis or fraud claim	YES	Patient level	NO	NO
T. Ekin, G. Lakomski, R. M. Musal(2019) L. Sun, C. Liu, C	NO	YES	NO	Provider level	YES	NO
A. Verma, A. Taneja, 2017	NO	Disease based	YES	Provider level	NO	NO
G. Liu, J. Guo, Y. Zuo, J. Wu, 2020 K. Malhotra, T. C. Hobson et al (2015)	NO	YES	YES	Provider level	NO	NO
Proposed framework	YES	NO	YES	Provider level, Patient level, service level	NO	YES

Table 8 Few generated rules

Speciality name	Rule
Pulmonologist	IF speciality is 'Pulmonologist' THEN service is Nebulizer Treatment 1-3Times "P" (0.08) OR Emergency Physician Charges (0.1) OR ESR (0.09) OR Rx Services - IPD (0.11) OR doc_04 - IPD Follow-up Visit (0.06) OR Intra Mascular /Subcu Injection (0.08) OR C-Reactive Protein(CRP) High Sensitivity (0.07) OR Urine C/S (0.08) OR Admission fee - Regular (0.06) OR doc_04 - IPD Initial Visit (0.07)
Neurosurgery	IF speciality is 'Neurosurgery ' THEN service is IV Cannula Insertion (0.05) OR Brain/Head (regular) (0.64) OR CBC Diff Profile (CS11) (0.09) OR Rx Services - IPD (0.11) OR Private Ward (0.02) OR Hip 2 Views (0.03) OR Emergency Services Charges(8pm onward) (0.13) OR doc_37 - IPD Initial Visit (0.72) OR Sodium Serum (1.0) OR Chest Xray 1 View (0.04) OR Emergency Physician Charges (0.1) OR doc_05 - IPD Follow-up Visit (0.02) OR Oxygen Administration 7-12 H "P" (0.92) OR Non Admissible Items (0.05) OR Nursing Care - Private Ward (0.03) OR Admission fee - Regular (0.06) OR Lumber Spine without Contrast (0.01) OR ECG 12 Lead (0.04) OR Medical Officer - Private Ward (0.04) OR Chem 7 (0.02) OR doc_37 - IPD Follow-up Visit (0.87) OR Potassium Serum (1.0)
Orthopedic	IF speciality is 'Orthopedic' THEN service is Blood C/S (Peads) (1.0) OR CBC Diff Profile (CS11) (0.09) OR Chem 7 (0.02) OR Non Admissible Items (0.05) OR APTT (0.02) OR HCT (1.0) OR doc_85 - IPD Initial Visit (0.35) OR IV Cannula Insertion (0.05) OR Admission fee - Regular (0.06) OR Glucose - POCT (0.01) OR doc_07 - IPD Follow-up Visit (0.02) OR Cardiac Profile (CPKMB, Troponin-I) (0.01) OR ORIF of trimalleolar fracture fixation (0.38) OR PT (Prothrombin Time) (0.02) OR Rx Services - IPD (0.11) OR doc_17 - IPD Follow-up Visit (0.17) OR Emergency Services Charges(8am - 8pm) (0.13) OR doc_85 - IPD Follow-up Visit (0.1) OR Operating Room (0.7) OR Hemoglobin (1.0) OR Chest Xray 1 View (0.04) OR Arterial Blood Gases (0.0) OR TSH (0.11) OR Emergency Physician Charges (0.1) OR doc_17 - IPD Initial Visit (0.1) OR C-Reactive Protein(CRP) High Sensitivity (0.07) OR Oxygen Administration 3 H "P" (0.07) OR Photo Therapy 24 H (0.01) OR Anesthetist Fee (0.67) OR ECG 12 Lead (0.04) OR CHEM-8 Profile - POCT (0.06)
Urologist	IF speciality is 'Urologist' THEN service is Lap.Assisted Orchidopexy(Ward/1Day) (0.64) OR Effusion - Cytology (1.0) OR doc_29 - IPD Follow-up Visit (0.3)

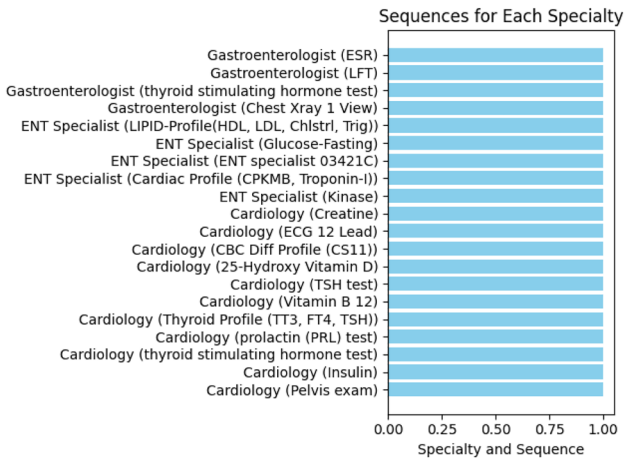

Fig. 11 Identified anomalous cases in a few specialities

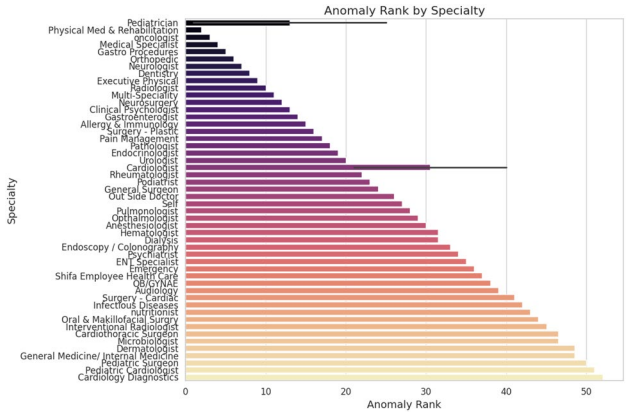

Fig. 12 Anomalies rank from all specialties after validation by the proposed framework

Figure 17 shows the tool's user interface, which we are implementing based on the proposed framework and methodology. There are 102 anomalies, and analysts will check all anomalous transactions and either accept them, reject them or put them in the pending list for further analysis. Additionally, we can see if a good number of declined transactions show a severe need for medical benefit optimisation and healthcare fraud detection.

The proposed framework can be implemented for any enterprise or hospital. The main task of our proposed framework is to detect the healthcare fraud with in insurance claim, once the rule engine and transformer detect anomalous transaction, it will be forwarded to analyst for more detailed analysis, when transaction is detected as a fraud then enterprise or hospital can take disciplinary action against the specific actors who are involved in the particular fraudulent transaction. The overall concept is depicted in the Fig. 18.

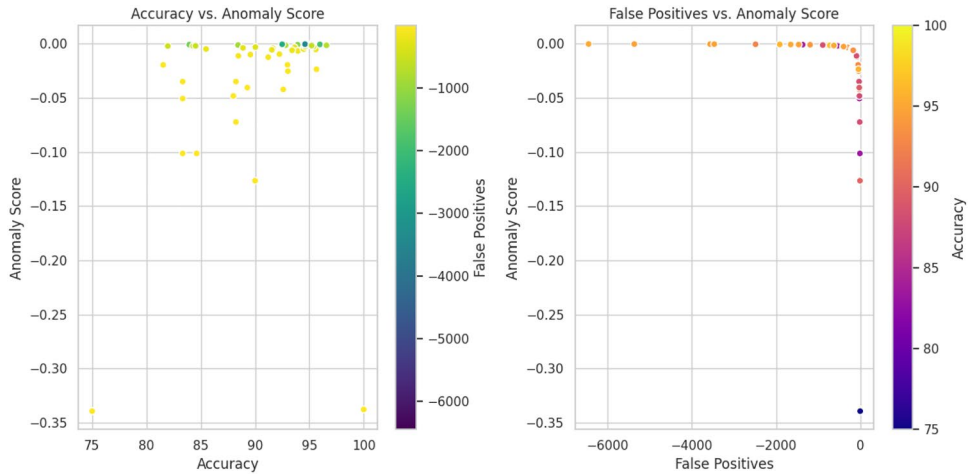

Fig. 13 Accuracy, anomaly score and false positive from all specialties after validation by the proposed framework

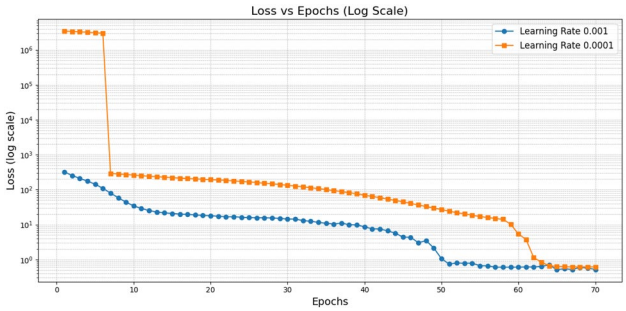

Fig. 14 Loss versus epochs

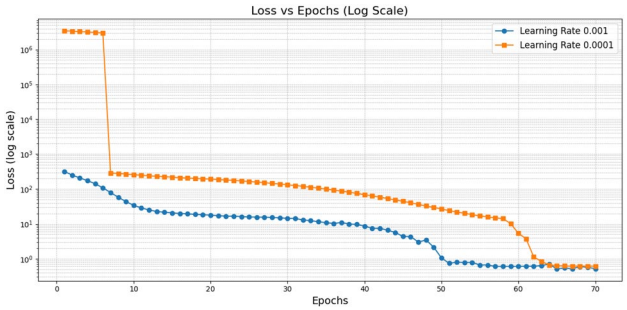

Fig. 15 Accuracy versus epochs

5 Discussion

We are detecting anomalies by using doctors (DOC_ID) and services (unique_service_id) - we want to find cases where a doctor performs a service or procedure that may not match their specialization. For comparison purposes, we have used the open-source dataset MIMIC-IV. The procedure events table in MIMIC-IV is the best choice for this task because:

- It contains information about the services or procedures provided to patients (just like unique_service_id in my dataset).
- It also includes the caregiver (doctor or nurse) who performed that procedure, similar to DOC_ID in our dataset.
- This matches our goal exactly - we want to find unusual or incorrect doctor-service assignments, and this table

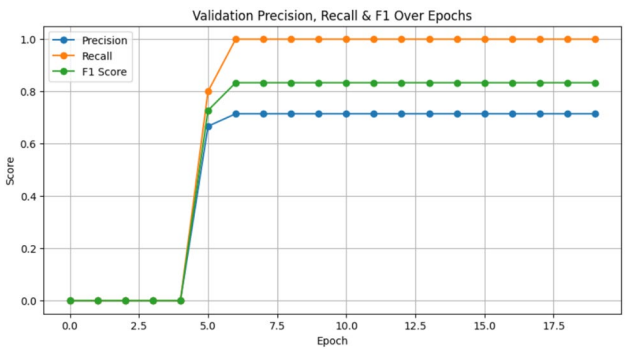

Fig. 16 Precision, recall and F1 score over epochs

Table 9 Performance evaluations of the proposed methodology

Performance metric	Value	Meaning
Accurac	0.97	97.49% of all predictions are correct
Precision	0.80	Out of all predicted anomalies, 80.77% were true anomalies (low false positives)
Recall	0.91	The model detected 91.3% of actual anomalies (low false negatives)
F1 Score	0.86	Harmonic mean of precision and recall, indicating balanced performance

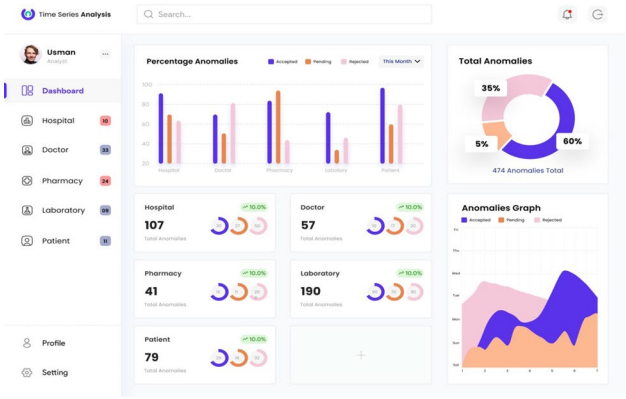

Fig. 17 Final interface for the analyst

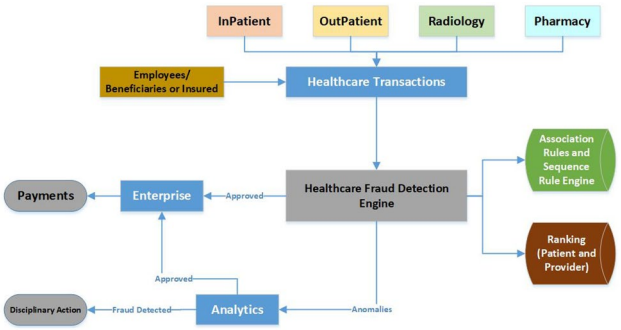

Fig. 18 Proposed framework implementation for any enterprise

"procedureevents" allows us to see which doctor performed which service.

- We can convert this data into sequences based on time or events, and apply the Anomaly transformer to detect patterns different from normal doctor-service relationships.

We use the Anomaly transformer on time-stamped caregiver-procedure data to detect unusual doctor-service combinations. By converting the sequences of procedures performed by each caregiver into a time series, the model learns normal patterns and flags deviations, helping uncover incorrect or suspicious assignments (Table 10).

Three main columns are used namely: caregiverid, itemid, and starttime, to generate a sequence of doctor-service actions over time. Using the proposed methodology, we have detected unusual doctor-service sequences.

Table 11 Generated anomalies in MIMIC IV

Timestamp	Caregiver ID	Item ID	Anomaly score
2111-01-17 14:58:00	97715.0	225,792	0.0965
2111-01-17 14:58:00	97715.0	225,469	0.1000
2111-01-17 14:58:00	97715.0	225,966	0.0966
2111-01-17 15:00:00	27016.0	225,752	0.0982
2111-01-17 15:00:00	27016.0	224,263	0.1073
2111-01-17 15:00:00	27016.0	224,277	0.1120
2111-01-17 15:00:00	27016.0	224,275	0.1009
2111-01-17 15:30:00	27016.0	225,459	0.1016
2111-01-17 16:03:00	27016.0	225,402	0.1005
2111-01-19 16:30:00	27016.0	227,712	0.0970

These flagged sequences in Table 11 represent procedure patterns that the model considered "unusual" or "unexpected" based on the training distribution. The anomalies could represent:

- Rare or unusual clinical procedures.
- Data entry errors.
- Edge cases or special treatment combinations.

For the sake of diversity, we have applied our proposed methodology to the MIMIC IV dataset, and we have observed that our model is performing well for this dataset as well.

The identified anomalies are depicted in Fig. 19. It can be observed that anomalies are mainly associated with rare itemids or unusual caregiver_id-itemid combinations. The proposed methodology has successfully flagged combinations that deviated from typical procedure sequences.

The transformeris a powerful but computationally intensive models, especially as model data and model size scale. The transformer needs hardware requirements such as GPU, RAM, Storage, Training time and Efficiency and software stacks such as PyTorch, TensorFlow frameworks are described in Table 12.

The proposed methodology can be extended by incorporating other features to facilitate fraud evaluation within the insurance management system. Since the dataset we have utilised to validate the current methodology included sensitive patient data, it was challenging to make it available. The dataset was in unstructured form, and it took a lot of time to

Table 10 Main columns of open source datatset

Column name	Description	Use in model
Starttime	Timestamp of when the procedure started	Time axis
Caregiver$_i d$	The ID of the doctor/nurse performing procedure	Like DOC$_I D$
Itemid	The procedure/service being performed	Like unique$_s ervice_i d$
Statusdescription	Status (e.g., FinishedRunning) - optional	Optional extra feature

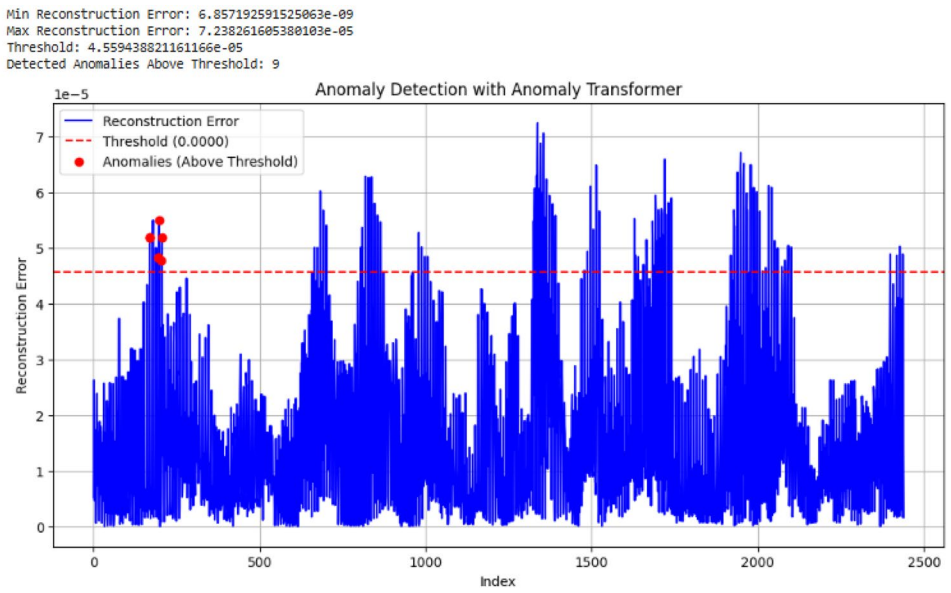

Fig. 19 Detected anomalies in MIMIC IV dataset

Table 12 System requirements for the proposed methodology

Resource	Minimum	Recommended
GPU	RTX 3060 / T4 (8–12 GB VRAM)	RTX 3090 / A100 (24–40 GB VRAM)
RAM	16 GB	32–64 GB
Disk	50 GB (SSD)	100 GB+ (SSD)
Extras	CUDA, PyTorch	Huggingface, mixed-precision

deal with the redundant and missing data. We utilised a five-year transactional dataset. However, larger datasets would be more beneficial and demonstrate the soundness of the suggested work from a wider angle and the usefulness of the framework and approach. Furthermore, the processing and storage of data will need to be moved to the cloud due to the large amount of data and its processing. When creating the fraud detection system, we considered age, gender, marital status, relationship, and frequency of visits. Expanding the suggested methodology by including additional features that can aid in assessing fraud is possible.

6 Conclusion

Our basic concern is the overburdened healthcare systems. The systems may become overburdened when doctors or other practitioners provide unnecessary treatments/ medications. Such unnecessary operations could waste resources and lead to a shortage of important medical supplies. Deserving and needy patients are not able to get access to the necessary healthcare resources or services. Existing research has made tremendous progress in identifying some fraud categories, but it hasn't given us a standardised method for identifying all forms of healthcare fraud. Our research, in contrast to earlier studies, focuses on using machine learning approaches to identify provider, patient, and service-level healthcare frauds in order to improve the efficiency and affordability of healthcare services. In the first section, a framework for detecting fraud is provided, including patients, physicians (providers), and services as its key components. Calculating association scores allows us to determine the connections between these components. The framework classifies fraud into provider, service, and patient-level fraud. By computing confidence values, this system also links each healthcare service to the relevant specialty. We have created a rule engine for detecting frauds by learning from previous transactional data. The dataset is first used to compute association scores among elements and then forwarded to the rule engine for analysis. After a rule engine examination, the fraud cases are ultimately located, and the ratings of all three components are updated. Additionally, we have used the Anomaly transformer to analyse the identified cases that have been detected. Patients' deviations from the normal sequences are identified as anomalous by analysing medical behaviours in clinical processes. Alternatively, it could be a less common behaviour. We can therefore identify sequences that deviate from common medical behaviours. The Anomaly transformer recognizes identifies the anomalous behaviors. The main contribution of our research is to implement a machine learning and deep learning based fraud detection system within the insurance management system. This has improved the overall performance of the system. The dataset was unstructured, and handling the duplicate

and missing data required a long time. We used a five-year transactional dataset, but larger datasets would be more helpful and show the value of the framework and approach and the soundness of the recommended work from a wider perspective. Additionally, because of the volume of data and its processing, the processing and storage of data will need to be moved to the cloud. We considered variables like age, gender, marital status, relationship, and frequency of visits when developing the fraud detection system. Actor-level frauds are detected, 50% are at the patient level, 13% are at the service versus patient level, 12% at the service versus doctor level and 25% are at the physician level. Further, these frauds are analysed by the Sequence rule engine based on the historical data. Once the frauds are identified our proposed architecture enables the management to take disciplinary action against each involved element.

T

Acknowledgements This project is funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R411), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Not applicable.

Data Availability The datasets are available from the corresponding author on reasonable request.

Declarations

Conflict of interest Authors have no conflict of interest.

References

Agarwal S (2023) An intelligent machine learning approach for fraud detection in medical claim insurance: a comprehensive study. Scholars J Eng Technol 11(9):191–200

Ahmad AYAB (2024) Fraud prevention in insurance: Biometric identity verification and ai-based risk assessment. In: 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), volume 1, pages 1–6

Alliance CH (2023) Commonwell health alliance. https://www.commonwellalliance.org

Altaf W, Shahbaz M, Guergachi A (2017) Applications of association rule mining in health informatics: a survey. Artif Intell Rev 47(3):313–340

Anbarasi M, Dhivya S (2017) Fraud detection using outlier predictor in health insurance data. In: 2017 International Conference on Information Communication and Embedded Systems (ICICES), pp 1–6. IEEE

Bara A, Botha I, Diaconita V, Lungu I, Velicanu A, Velicanu M (2009) A model for business intelligence systems' development. Inf Econ 13(4):99

Baran B (1987) The technological transformation of white-collar work: a case study of the insurance industry. Comput Chips Pap Clips 2:25–62

Bauder RA, Khoshgoftaar TM (2016a) A novel method for fraudulent medicare claims detection from expected payment deviations (application paper). In: 2016 IEEE 17th international conference on information reuse and integration (IRI), pp. 11–19, IEEE

Bauder RA, Khoshgoftaar TM (2016b) A probabilistic programming approach for outlier detection in healthcare claims. In: 2016 15th IEEE international conference on machine learning and applications (ICMLA), pp 347–354, IEEE

Bauder RA, Khoshgoftaar TM (2018) The detection of medicare fraud using machine learning methods with excluded provider labels. In: The Thirty-First International Flairs Conference

Bauder RA, Khoshgoftaar TM, Richter A, Herland M (2016). Predicting medical provider specialties to detect anomalous insurance claims. In: 2016 IEEE 28th international conference on tools with artificial intelligence (ICTAI), pp 784–790, IEEE

Bieberstein N (2006) Service-oriented architecture compass: business value, planning, and enterprise roadmap. FT Press

Cai R, Liu M, Hu Y, Melton BL, Matheny ME, Xu H, Duan L, Waitman LR (2017) Identification of adverse drug-drug interactions through causal association rule discovery from spontaneous adverse event reports. Artif Intell Med 76:7–15

Carta S, Fenu G, Recupero DR, Saia R (2019) Fraud detection for e-commerce transactions by employing a prudential multiple consensus model. J Inf Secur Appl 46:13–22

Chandola V, Sukumar SR, Schryver JC (2013) Knowledge discovery from massive healthcare claims data. In: Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining, pp 1312–1320, ACM

Corporation C (2023a) Cerner electronic health records. https://www.cerner.com

Corporation ES (2023b) Epic electronic health records. https://www.epic.com

Cui H, Li Q, Li H, Yan Z (2016) Healthcare fraud detection based on trustworthiness of doctors. In: 2016 IEEE Trustcom/BigDataSE/ISPA, pp 74–81, IEEE

Ekin T, Lakomski G, Musal RM (2019) An unsupervised bayesian hierarchical method for medical fraud assessment. Stat Anal Data Min: ASA Data Sci J 12(2):116–124

Eling M, Nuessle D, Staubli J (2022) The impact of artificial intelligence along the insurance value chain and on the insurability of risks. The Geneva Papers on Risk and Insurance-Issues and Practice 47(2):205–241

Feldman K, Chawla NV (2015) Does medical school training relate to practice? evidence from big data. Big data 3(2):103–113

Gath I, Geva AB (1989) Unsupervised optimal fuzzy clustering. IEEE Transactions on Pattern Analysis & Machine Intelligence 7:773–780

Gupta M, Gao J, Aggarwal C, Han J (2014) Outlier detection for temporal data. Synthesis Lectures on Data Mining and Knowledge Discovery 5(1):1–129

Herland M, Bauder RA, Khoshgoftaar TM (2017). Medical provider specialty predictions for the detection of anomalous medicare insurance claims. In *2017 IEEE International Conference on Information Reuse and Integration (IRI)*, pages 579–588. IEEE

Hristidis V (2009) Information discovery on electronic health records. CRC Press

Huang Z, Lu X, Duan H (2012). Anomaly detection in clinical processes. In *AMIA Annual Symposium Proceedings*, volume 2012, page 370. American Medical Informatics Association

Itri B, Mohamed Y, Mohammed Q, Omar B (2019). Performance comparative study of machine learning algorithms for automobile insurance fraud detection. In *2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS)*, pages 1–4. IEEE

Ivan M-L (2014). Characteristics of in-memory business intelligence. *Informatica Economica*, 18(3)

Joudaki H, Rashidian A, Minaei-Bidgoli B, Mahmoodi M, Geraili B, Nasiri M, Arab M (2015) Using data mining to detect health care fraud and abuse: a review of literature. Global J Health Sci 7(1):194

Jr JBH, Tobin CE (2020) The false claims act and government healthcare programs: A comprehensive guide to legal liability. Journal of Health Law and Policy 12(3):145–165

Köppen M, Kasabov N, Coghill G (2009) Advances in Neuro-Information Processing: 15th International Conference, ICONIP 2008, Auckland, New Zealand, November 25–28, 2008, Revised Selected Papers, vol 5507. Springer

Kose I, Gokturk M, Kilic K (2015) An interactive machine-learning-based electronic fraud and abuse detection system in healthcare insurance. Appl Soft Comput 36:283–299

Kowshalya G, Nandhini M (2018). Predicting fraudulent claims in automobile insurance. In *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pages 1338–1343. IEEE

Lenard MJ, Alam P (2005). Application of fuzzy logic to fraud detection. In *Encyclopedia of Information Science and Technology, First Edition*, pages 135–139. IGI Global

Li J, Huang K, Jin J, Shi J (2008) A survey on statistical methods for health care fraud detection. Health Care Manag Sci 11(3):275–287

Liu G, Guo J, Zuo Y, Wu J, Guo R-y (2020). Fraud detection via behavioral sequence embedding. *Knowledge and Information Systems*, pages 1–24

Liu J, Bier E, Wilson A, Guerra-Gomez JA, Honda T, Sricharan K, Gilpin L, Davies D (2016) Graph analysis for detecting fraud, waste, and abuse in healthcare data. AI Mag 37(2):33–46

Liu Q, Vasarhelyi M (2013). Healthcare fraud detection: A survey and a clustering model incorporating geo-location information. In *29th world continuous auditing and reporting symposium (29WCARS), Brisbane, Australia*

Matloob I, Khan S, Hussain F et al (2020) Medical health benefit management system for real-time notification of fraud using historical medical records. Appl Sci 10(15):5144

Matloob I, Khan SA, Rahman HU (2020) Sequence mining and prediction-based healthcare fraud detection methodology. IEEE Access 8:143256–143273

Kaushik Keshav, Akashdeep Bhardwaj, Ashutosh Dhar Dwivedi, Rajani Singh (2022) "Machine learning-based regression framework to predict health insurance premiums." *International Journal of Environmental Research and Public Health* 19, no. 13 : 7898

Vuddanti Sowjanya, VGSK Rishi Kumar Jamili, Sadhvik Reddy Bommareddy, Vivek Rotta, and Vamsi Pagadala (2024) "Machine Learning Insights into Personalized Insurance Pricing." In *2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, pp. 923–927. IEEE,

Jyothsna, Chaparala, K. Srinivas, Bandi Bhargavi, Akuri Eswar Sravanth, Atmuri Trinadh Kumar, JNVR Swarup Kumar (2022) "Health insurance premium prediction using XGBoost Regressor." In *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, pp. 1645–1652. IEEE

Fursov I, Kovtun E, Rivera-Castro R, Zaytsev A, Khasyanov R, Spindler M, Burnaev E (2022) Sequence embeddings help detect insurance fraud. IEEE Access 10:32060–32074

Mavundla Khulekani, Surendra Thakur, Emmanuel Adetiba, Abdultaofeek Abayomi (2024) "Predicting Cross-Selling Health Insurance Products Using Machine-Learning Techniques." *Journal of Computer Information Systems* : 1–18

Dey R, Roy A, Akter J, Mishra A, Sarkar M (2025) AI-driven machine learning for fraud detection and risk management in US healthcare billing and insurance. Journal of Computer Science and Technology Studies 7(1):188–198

Zhang Guoming, Zhang Xuyun, Bilal, Muhammad, Dou, Wanchun, Xu, Xiaolong,Rodrigues, Joel JPC (2022) "Identifying fraud in medical insurance based on blockchain and deep learning." *Future Generation Computer Systems*, vol. 130, pp. 140–154, Elsevier

MEDITECH (2023). Clinical decision support systems. https://www.meditech.com

Musal RM (2010) Two models to investigate medicare fraud within unsupervised databases. Expert Syst Appl 37(12):8628–8633

Okita A, Yamashita M, Abe K, Nagai C, Matsumoto A, Akehi M, Yamashita R, Ishida N, Seike M, Yokota S et al (2009) Variance analysis of a clinical pathway of video-assisted single lobectomy for lung cancer. Surg Today 39(2):104–109

Ou-Yang C, Agustianty S, Wang H-C (2013) Developing a data mining approach to investigate association between physician prescription and patient outcome-a study on re-hospitalization in stevens-johnson syndrome. Comput Methods Programs Biomed 112(1):84–91

Palmer JH, Carter SM (2021) Misuse and fraud in the u.s. medicaid program: A case study of systemic challenges and policy responses. Journal of Health Policy and Management 14(2):133–145

Peng J, Li Q, Li H, Liu L, Yan Z, Zhang S (2018). Fraud detection of medical insurance employing outlier analysis. In *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))*, pages 341–346. IEEE

Ramalingam S, Subramanian M, Sreevallabha Reddy A, Tarakaramu N, Ijaz Khan M, Abdullaev S, Dhahbi S (2024) Exploring business intelligence applications in the healthcare industry: A comprehensive analysis. Egyptian Informatics Journal 25:100438

Reis T, Kreibich A, Bruchhaus S, Krause T, Freund F, Bornschlegl MX, Hemmje ML (2022) An information system supporting insurance use cases by automated anomaly detection. Big Data and Cognitive Computing 7(1):4

Savino JO, Turvey BE (2018). Medicaid/medicare fraud. In *False Allegations*, pages 89–108. Elsevier

Seo J, Mendelevitch O (2017). Identifying frauds and anomalies in medicare-b dataset. In *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 3664–3667. IEEE

Sowah RA, Kuuboore M, Ofoli A, Kwofie S, Asiedu L, Koumadi KM, Apeadu KO (2019). Decision support system (dss) for fraud detection in health insurance claims using genetic support vector machines (gsvms). *Journal of Engineering*, 2019

Subudhi S, Panigrahi S (2017). Use of optimized fuzzy c-means clustering and supervised classifiers for automobile insurance fraud detection. *Journal of King Saud University-Computer and Information Sciences*

Thornton D, Mueller RM, Schoutsen P, Van Hillegersberg J (2013) Predicting healthcare fraud in medicaid: a multidimensional

data model and analysis techniques for fraud detection. Procedia Technol 9:1252–1264

Thornton D, van Capelleveen G, Poel M, van Hillegersberg J, Mueller RM (2014) Outlier-based health insurance fraud detection for us medicaid data. In ICEIS 2:684–694

Ortega PA, Figueroa CJ, Ruz GA (2006) A Medical Claim Fraud/Abuse Detection System based on Data Mining: A Case Study in Chile. DMIN 6:26–29

Toti G, Vilalta R, Lindner P, Lefer B, Macias C, Price D (2016) Analysis of correlation between pediatric asthma exacerbation and exposure to pollutant mixtures with association rule mining. Artif Intell Med 74:44–52

Travaille P, Müller RM, Thornton D, Van Hillegersberg J (2011). Electronic fraud detection in the us medicaid healthcare program: Lessons learned from other industries. In *AMCIS*

Van de Klundert J, Gorissen P, Zeemering S (2010) Measuring clinical pathway adherence. J Biomed Inform 43(6):861–872

Verma A, Taneja A, Arora A (2017). Fraud detection and frequent pattern matching in insurance claims using data mining techniques. In *2017 Tenth International Conference on Contemporary Computing (IC3)*, pages 1–7. IEEE

Vinora A, Surya V, Lloyds E, Kathir Pandian B, Deborah RN, Gobinath A (2023). An efficient health insurance prediction system using machine learning. In *2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, pages 1–5

Vosseler A (2022). Unsupervised insurance fraud prediction based on anomaly detector ensembles. *Risks*, 10(7)

Wells JT (2019) Healthcare fraud: Understanding and combating provider and patient schemes. J Forensic Investig Account 11(1):23–40

Yang W-S, Hwang S-Y (2006) A process-mining framework for the detection of healthcare fraud and abuse. Expert Syst Appl 31(1):56–68

Yang W-S, Hwang S-Y (2006) A process-mining framework for the detection of healthcare fraud and abuse. Expert Syst Appl 31(1):56–68

Zafari B, Ekin T (2019) Topic modelling for medical prescription fraud and abuse detection. J Roy Stat Soc: Ser C (Appl Stat) 68(3):751–769

Zeng L, Wang B, Fan L, Wu J (2016) Analyzing sustainability of chinese mining cities using an association rule mining approach. Resour Policy 49:394–404

Li W, Zhang H, Chen M (2025) A short-term wind power prediction method via self-adaptive spatiotemporal graph neural networks. Computers & Electrical Engineering 110:110106

Li W, Zhang H, Chen M (2025) A short-term wind power prediction method via self-adaptive spatiotemporal graph neural networks. Computers & Electrical Engineering 110:110106

Hekmat A, Li Z (2024) An attention-fused architecture for brain tumor diagnosis. Biomed Signal Process Control 101:107221

Zhang L, Wang Q, Liu Y (2024) Adaptive decision-making with deep Q-network for heterogeneous UAV swarms. Appl Soft Comput 150:112366

Khan MA, Khan S, Haider S, Khan SA, Bilal O (2024) Evolving knowledge representation learning with the dynamic asymmetric embedding model. Evol Syst 6:2323–2338

Alrawili T, Alzahrani B, Khan MA (2025) Comprehensive survey: Biometric user authentication application, evaluation, and discussion. J Netw Comput Appl 220:103652

Arif F, Mehmood R, Katib I, Albeshri A (2024) Towards Efficient Energy Utilization Using Big Data Analytics in Smart Cities for Electricity Theft Detection. IEEE Access 12:11845–11859

Si-Ahmed L, Hafid A, Samhat AE (2024) Survey of Machine Learning based intrusion detection methods for Internet of Medical Things. Comput Netw 245:110947

Khan S, Ali H, Ahmad I, Shah MA, Lee S (2024) Evolving knowledge representation learning with the dynamic asymmetric embedding model. Knowl-Based Syst 294:110309