

Survey Paper on Fraud detection in Healthcare using Deep Learning

¹Pooja Kushwaha, ²Prof. Hitesh Gupta

M. Tech Scholar, Department of Computer Science and Engineering, LNCT, Bhopal¹

Assistant Professor, Department of Computer Science and Engineering, LNCT, Bhopal²

Abstract: - Healthcare is an essential in people's lives and it must be affordable. The healthcare industry is an intricate system with numerous moving components. It is expanding at an expeditious pace. At the same time, fraud in this industry is turning into a critical problem. One of the issues is the misuse of the medical insurance systems. Manual detection of frauds in the healthcare industry is a strenuous work. Recently, machine learning and data mining techniques are used for automatically detecting the healthcare frauds. In this paper, we attempt to give a review on frauds in healthcare industry and the techniques for detecting such frauds. With an emphasis on the techniques used, determining the significant sources and the features of the healthcare data, various available researches were studied in the literature work. From this review it can be concluded that the advanced machine learning techniques and incipiently acquired sources of the healthcare data would be forthcoming subjects of interest in order to make the healthcare affordable, to improve the effectiveness of healthcare fraud detection and to bestow top quality on healthcare systems. Many recent researches, as reviewed in this paper, use machine learning and deep learning to detect fraud in healthcare industry. There is a need additional research work to determine different unusual patterns of misuse of health insurance systems and more sophisticated machine learning techniques can be used to improve results.

Keywords: - Fraud Detection, Deep Learning, Healthcare

I. INTRODUCTION

Medical care has and propagates to be a vital part in individuals' lives. The human body is a compound design. As a result, it is essential to have specialist doctors who are qualified to diagnose and treat diseases in various body parts. Because of this, doctors in various specialties perform a variety of treatment procedures on patients. Serving as many patients as possible with success is the industry's goal. However, there is a cost associated with each treatment and service. Various medical facilities, as well as physicians, drug dealers, and medical staff, must be compensated for their time and expertise. Regularly these costs are not reasonable to the patients. As a result, insurance plans are used to spread out costs among all healthcare patients and pay for the necessary staff and equipment. There is a possibility of misuse or fraud, as with any insurance system [1, 2].

Healthcare fraud is becoming increasingly recognized as a serious social issue. There is no doubt that healthcare fraud is a problem for the government, and more efficient methods of detection are required. It takes a lot of effort and extensive medical knowledge to identify healthcare fraud [3].

Healthcare fraud detection has traditionally relied heavily on the expertise of domain experts, which is incorrect, costly, and time-consuming. A few auditors must manually review and identify suspicious medical insurance claims in order to perform manual healthcare fraud detection, which takes a lot of time and effort. However, more effective and automated methods for detecting healthcare fraud have emerged as a result of recent advancements in machine learning and data mining [4, 5]. There has been a developing interest in digging medical services information for misrepresentation discovery in the ongoing years. This paper surveys the different methodologies utilized for distinguishing the deceitful exercises in Health care coverage guarantee information.

II. LITERATURE REVIEW

John T. Hancock et al. [1], use an innovative ensemble supervised feature selection method to create explainable machine learning models for Big Data. The method is applied to the Medicare public health insurance program's publicly available insurance claims data. Through the classification of highly imbalanced Big Data, we approach Medicare insurance fraud detection as a supervised machine learning task of anomaly detection. The improvement of model training efficacy and the creation of machine learning models for fraud detection that are more explainable are our goals for feature selection. We demonstrate how our feature selection method reduces the dimensionality of two Big Data datasets derived from two distinct sources of insurance claims data by approximately 87.5 percent without sacrificing performance.

In addition, machine learning models with reduced dimensionality are simpler to explain and less prone to overfitting. As a result, our primary contribution to the field of application of automated Medicare insurance fraud detection is the demonstration of our novel feature selection method. We explain our fraud detection models in terms of the definitions of the selected features by utilizing our feature selection technique. Any set of machine learning algorithms that keep a list of feature

importance values can be used with the ensemble supervised feature selection method we present. Subsequently, specialists may effectively utilize varieties of the strategy we present.

Eman Nabrawi et al. [2], medical services misrepresentation is purposefully submitting misleading cases or creating confusion of realities to acquire qualification installments. As a result, it increases healthcare costs and wastes resources. As a result, fraud is a significant financial challenge. Hence, administered machine and profound learning investigation like arbitrary backwoods, calculated relapse, and fake brain networks are effectively used to identify medical care protection extortion. The goal of this study is to create a health model that can automatically spot fraud in Saudi Arabian health insurance claims. The model shows the best contributing element to misrepresentation with ideal exactness. Three supervised deep and machine learning techniques were utilized in the labeled imbalanced dataset. The dataset was gotten from three medical services suppliers in Saudi Arabia. Random forest, logistic regression, and artificial neural networks were the models used. The SMOT strategy was utilized to adjust the dataset. Insignificant features were excluded using Boruta object feature selection. Accuracy, precision, recall, specificity, F1 score, and area under the curve (AUC) were the validation metrics. Arbitrary woods classifiers demonstrated approach type, instruction, and mature as the main highlights with an exactness of 98.21%, 98.08% accuracy, 100 percent review, a F1 score of 99.03%, particularity of 80%, and an AUC of 90.00%. The accuracy of logistic regression was 80.36%, the precision was 97.62%, the recall was 80.39%, the F1 score was 88.17%, the specificity was 80%, and the AUC was 80.20%. ANN uncovered an exactness of 94.64%, 98.00% accuracy, 96.08% review, a F1 score of 97.03%, an explicitness of 80%, and an AUC of 88.04%. The three successful models used in this study of predictive analytics each produced acceptable accuracy and validation metrics; However, additional investigation using a larger dataset is recommended.

Mayaki et al. [3], medicare fraud results in higher client premiums and significant losses for governments and insurance companies. In the United States, Medicare fraud costs between 21 billion and 71 billion dollars per year, while it costs around 13 billion euros in Europe. The goal of this study is to use classifiers based on artificial neural networks to predict Medicare fraud. The highly imbalanced data sets present the primary challenge when employing machine learning techniques for fraud detection or, more broadly, anomaly detection. We propose a classifier based on multiple inputs and based on a deep neural network with a Long-short Term Memory (LSTM) autoencoder to identify Medicare fraud. This architecture facilitates the final model's classification task by allowing it to take into account a variety of data sources without combining them. The dormant elements extricated from the LSTM autoencoder have major areas

of strength for a power and separate the suppliers into homogeneous bunches. We make use of the sets of data that come from the US federal government's Centers for Medicare and Medicaid Services (CMS). The CMS gives freely accessible information that unites all of the expense cost demands sent by American clinics to government health care organizations. Our findings demonstrate that our multiple inputs neural networks outperform baseline artificial neural networks, despite their superior performance. We have demonstrated that embedding provider behavior with a LSTM autoencoder improves outcomes and strengthens classifiers against class imbalance.

Salekshahrezaee et al. [4], it is innately difficult to prepare an AI calculation on a class-imbalanced dataset. Due to the large number of features in the dataset, this training process may become even more challenging in high-dimensionality conditions. Data sampling and feature extraction are frequently used to reduce the number of dataset features during preprocessing to address class imbalance. In this review, we investigate the utilization of these two preprocessing exercises prior to giving the information to four troupe classifiers (Arbitrary Woodland, CatBoost, LightGBM, and XGBoost). The Principal Component Analysis (PCA) and Convolutional Autoencoder (CAE) approaches are evaluated with regard to feature extraction. The Random Undersampling (RUS) and Synthetic Minority Oversampling Technique (SMOTE) approaches to data sampling are evaluated. The Area Under the Receiver Operating Characteristic Curve (AUC) metric measures classification performance. Based on our findings, the CAE method, followed by the RUS method, provides the best classification performance.

Sailaja et al. [5], there is an overall rise in the number of elderly people and the associated costs and medical requirements. Medicare is a health insurance program in the United States that helps people over 65 with some of the costs of medical care by providing coverage. Despite this, healthcare expenses are high and will continue to rise. Healthcare costs are rising due in large part to fraud. A comprehensive investigation using machine learning techniques to identify fraudulent Medicare providers is presented in our paper. In order to construct and evaluate three distinct learners, we make use of provider exclusions for fraud labels and publicly accessible Medicare data. Given the low number of actual fraud labels, we employ random under sampling to generate four class distributions in order to lessen the impact of class imbalance. With average AUC scores of 0.883 and 0.882, respectively, and low false negative rates, our findings demonstrate that the C4.5 decision tree and logistic regression learners have the best fraud detection performance, particularly for the 80:20 class distribution. We successfully demonstrate how machine learning and random under sampling can be used to identify Medicare fraud.

Gupta RY et al. [6], due to the financial consequences of fraud, which include costs associated with investigations,

revenue losses, and reputational risk, fraud detection is an important area of healthcare system research. The majority of businesses use fraud detection models based on Machine Learning or Deep Learning to mitigate this. Productive misrepresentation identification models work on the exhibition of medical services frameworks. Data imbalance is one of the main obstacles in building an effective fraud detection model: skewed proportion of less fraudulent cases compared to cases that were not fraudulent. Choosing a classification model: use of appropriate deep learning or machine learning models to identify fraud or non-fraud cases. In this work, we have overcome these obstacles by utilizing six classification models and three distinct data-imbalance techniques; we have likewise utilized six variations of brain network models. For this, we have utilized information from area of the planet biggest general wellbeing inclusion plot called Ayushman Bharat (PM-JAY India). In total, 26 models were evaluated as part of this study. Accuracy, sensitivity, specificity, and the F1-score were some of the various metrics that were used to evaluate these models' performance. In this study, it was found that a neural network model trained on data that was undersampled performed better than other models.

Karmiani et al. [7], prediction is a complicated process due to the stock market's variation and dependence on various parameters. Counterfeit brain Organizations have been shown to be helpful in such cases to foresee the stock qualities. The boundaries in question and the ordinarily utilized calculations are examined and analyzed in this paper. In the event of backpropagation calculation, a feed forward network is available and loads are changed by back spreading the mistake. In a similar vein, a significant change is made to the Support Vector Machines Algorithm (SVMA), which improves accuracy rates. It is more adaptable due to the kernel and other parameters' presence. Long Transient Memory (LSTM), another usually utilized time series determining calculation, is an extraordinary sort of Repetitive Brain Network(RNN) that utilizes inclination plunge calculation. On the basis of accuracy, variation, and time required for various numbers of epochs, this paper compares these algorithms. The reliability of each algorithm was further evaluated with the T-test hypothesis test.

Bauder et al. [8], there is a lot of data generated in the healthcare industry. Patient records and provider payments are included in this big data. In areas like fraud detection, the use of big data is frequently regarded as the most effective approach. We show in this study that using more highly imbalanced big data does not yield satisfactory results for fraud detection. Seven distinct class distributions are generated using random undersampling, and performance results are compared. The actual fraud labels from the List of Excluded Individuals/Entities (LEIE) are mapped using the Medicare Provider Utilization and Payment Data for the calendar years 2012–2015. Based on building Random Forest models with 5-fold cross-validation, our findings show that the best class

distribution, 90:10, has an AUC of 0.87302, while the worst fraud detection performance was achieved by the balanced and two highly imbalanced distributions. In addition, we demonstrate that employing a 99:1 (imbalanced) class distribution was significantly superior to the commonly used ratio of 50:50 (balanced). Our research indicates that the 50:50 class distribution does not provide the best results for Medicare fraud detection and clearly demonstrates the necessity of sampling big data with class imbalance.

Chen et al. [9], the act of knowingly submitting false claims or misrepresenting a fact in order to obtain a federal health care payment for which no entitlement would otherwise exist is considered fraud. Medicare and Medicaid fraud are commonplace in today's health care system. Because it diverts resources meant to care for patients in need to the benefit of fraudsters, fraud has a significant negative impact. Beneficiaries of Medicare and Medicaid may suffer harm as a result of fraud's potential to raise overall costs for essential health care services. This commentary's goals are to provide suggestions for safeguarding patients and health care practices as well as a description of the various types and trends of Medicare and Medicaid fraud. This article focuses on the beneficiary (patient) and provider levels of Medicare and Medicaid fraud, which can be intentional or unintentional. In addition, the Stark Law, the False Claims Act, and the Anti-Kickback Statute are all discussed in this article, along with examples of fraud that are relevant to each law. We also talk about emerging and trending topics like pharmacogenetic and opioid testing; In today's health care landscape, both have experienced fraud in greater numbers and with greater public profile. Last but not least, the article provides a synopsis of fraud detection techniques and advice for health care providers and patients on how to protect themselves from it. At the policy, practice, and grassroots levels, recommended strategies to combat fraud are discussed. Medical care specialists, including drug specialists, can utilize these techniques to shield themselves and their patients from becoming casualties of misrepresentation or unwittingly committing extortion.

Herland M et al. [10], the general well-being of the population in the United States continues to rise as a result of advancements in technology and medical science. Programs like Medicare are needed to help manage the high costs of high-quality healthcare as this progress continues. The inability of Medicare to effectively meet the healthcare requirements of the elderly and other qualifying individuals is hampered by the presence of individuals who engage in fraud for the purpose of nefarious motives and personal gain. The Centers for Medicare and Medicaid Services (CMS) have made a number of "Big Data" datasets available for various parts of the Medicare program in an effort to reduce fraudulent activities. Using the following CMS datasets, we focus on Medicare fraud detection in this paper: 1) Federal medical insurance Supplier Use and Installment Information: (2) Medicare Provider Utilization and Payment Data:

Physician and Other Supplier (Part B) Part D Prescriber (Part D), and (3) Government medical care Supplier Usage and Installment Information: Referring to Supplies, Prosthetics, and Durable Medical Equipment (DMEPOS). Additionally, we combine the three primary datasets to create a fourth dataset. The mapping of real-world provider fraud labels using the Office of the Inspector General's List of Excluded Individuals and Entities (LEIE) is the subject of our discussion, as is data processing for each of the four datasets. Three learners are built and evaluated for each dataset in our exploratory analysis of Medicare fraud detection. Our findings indicate that the combined dataset with the Logistic Regression (LR) learner had the highest overall score, with a value of 0.816, followed closely by the Part B dataset with LR, with a value of 0.805. This performance metric is called the Area under the Receiver Operating Characteristic (ROC) Curve. Generally, the Consolidated and Part B datasets created the best extortion identification execution with no factual distinction between these datasets, over every one of the students. We recommend using the Combined dataset to detect fraudulent behavior when a physician has submitted payments through any or all Medicare parts evaluated in our study, based on our findings and the assumption that there is no way to know which part of Medicare a physician will commit fraud.

III. DEEP LEARNING

Deep learning is a subset of machine learning and artificial intelligence (AI) that uses artificial neural networks to model and solve complex problems. It mimics the way the human brain operates when processing information, allowing machines to learn from large datasets with minimal human intervention. The goal of machine learning (ML) algorithms is to move forward without human intervention. Since insight is based on learning, ML is an essential part of computerized reasoning [14, 15]. There are various types of ML methods, for example,

Supervised Instruction: - Predictions are made for specific data samples by these algorithms. The section is framing information and marks known as spam or non-spam. A model is prepared by a planning technique; They are constructed in gauges and revisions on the assumption that these expectations are false. This readiness strategy continues until the model achieves the crucial precision of the arrangement data (as shown in Fig. 1).



Fig 1: Supervised Learning

SVM: - This is for issues with arrangement and relapse. SVM organizes data into different classes by recognizing a hyperplane (line) that disconnects getting ready data into classes. The likelihood of summing up imperceptible information increases when the hyperplane that increases

the distance between classes is recognized [16]. SVM offers the best portrayal execution, for instance the accuracy of the readiness set. It doesn't flood the data. SVM is in a general sense used for expecting time series assessment. SVM has no solid suspicions regarding the data. Show greater efficiency for the right gathering of future data. SVM is organized into two orders, for instance Straight and non-direct. Preparing data is addressed by an isolated line, such as a hyperplane, in a straight methodology.

RF: - RF ML estimations are prepared for performing both backslide and arrange tasks. In RF technique a couple of decision trees are outlined and computation combines the rules of these decision trees and conveys company learning rules for estimate. The model produces precise results by utilizing a collection of these choice trees because it is designed with in-depth and distinct expert knowledge of a few choice trees [7].

IV. DEEP LEARNING APPROACH

The profound dis-criminative models incorporate DNNs, RNNs, CNNs. RBMs, DBNs, DBMs, and DA are the generative/unsupervised models. There are three main classes of Deep learning techniques that can be used depending on how they are going to be used: 1) Deep networks for unsupervised or generative learning; 2) Profound organizations for administered learning; also, 3) Mixture profound organizations. IDs currently lack full perfection. Regarding IDS, there is a great deal of issues. Few of the gaps are inherent in the way IDSs are created, but as these IDSs develop, several of them are frequently filled by enhancing and processing existing methodologies.

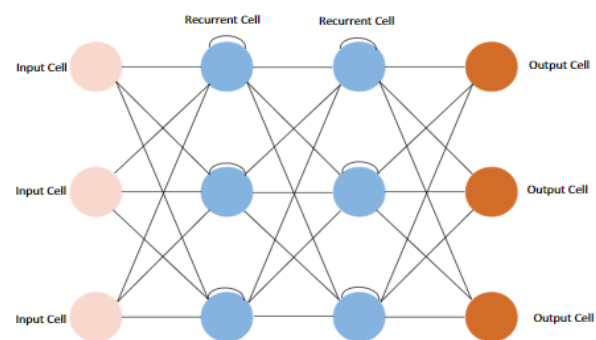


Figure 2: Recurrent neural network

4.1 Multi-facet Perceptron (MLP)

An IDS just detects attacks; it does not halt or block them. Because of this, associate IDS should be a part of a full setup that includes other security measures and personnel who are trained to respond appropriately. IDSs are particularly useful for network viewing. However, how useful they are relying on what you do with the information you give them. Because discovery technologies don't prevent or address possible problems, they are useless when you increase security unless you have the right personnel and processes in place to handle

them and respond to threats. Because an IDS is unable to detect them, hackers will utilise them to access the network. Only because they are more severe within the network does an IDS register these attacks. Systems remain exposed as a result until the assault is discovered. This is a major drawback because it makes encryption much more required to protect our information.

4.2 Convolutional Neural Network (CNN, also known as ConvNet)

Regularized MLP networks and other traditional ANNs benefit from the CNN's design enhancements. In addition to simplifying the model, each CNN layer takes into account the best parameters for producing a meaningful output. Additionally, CNN employs a "dropout" that is capable of addressing the issue of over-fitting, which may arise on a conventional network. The capacity of consequently finding fundamental highlights from the contribution without the requirement for human mediation makes it more remarkable than a conventional organization. In the field, there are a number of variations of CNN, such and others that, depending on how well they learn, can be used in a variety of application fields. One of the main drawbacks of an IDS is that false positives are constantly alerted about. False positives are more common than actual threats in many instances. To lessen the number of false alarms, an IDS is altered. Your technicians need time to respond, though. False alerts could disrupt or be ignored during true attacks if they don't manage them

4.3 The Recurrent Neural Network (RNN) and Its Variants

Repetitive organizations gain from preparing input, notwithstanding, recognize by their "memory", which permits them to affect current information and result through utilizing data from past information sources. Dissimilar to run of the mill DNN, which expects that data sources and results are free of each other, the result of RNN is dependent on earlier components inside the succession. However, the problem of vanishing gradients in standard recurrent networks makes it difficult to learn long data sequences. We'll go over a few well-known variations of the recurrent network that perform well in a wide range of real-world application domains and minimize the issues.

V. METHODOLOGY

In this paper new solutions that overcome aforementioned challenges in fraud detection in healthcare system strategy adopt the long short term memory (LSTM) technique.

Long Short-Term Memory (LSTM) is one of many types of Recurrent Neural Network RNN, it's also capable of catching data from past stages and use it for future predictions.

In general, an Artificial Neural Network (ANN) consists of three layers: 1) input layer, 2) Hidden layers, 3) output layer.

In a NN that only contains one hidden layer the number of nodes in the input layer always depend on the dimension of the data, the nodes of the input layer connect to the hidden layer via links called 'synapses'.

The relation between every two nodes from (input to the hidden layer), has a coefficient called weight, which is the decision maker for signals.

The process of learning is naturally a continues adjustment of weights, after completing the process of learning, the Artificial NN will have optimal weights for each synapses.

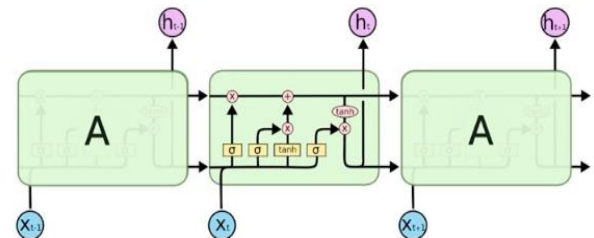


Figure 3: The internal structure of an LSTM

The principal component of LSTM is the cell state. To add or remove information from the cell state, the gates are used to protect it, using sigmoid function (one means allows the modification, while a value of zero means denies the modification.). We can identify three different gates:

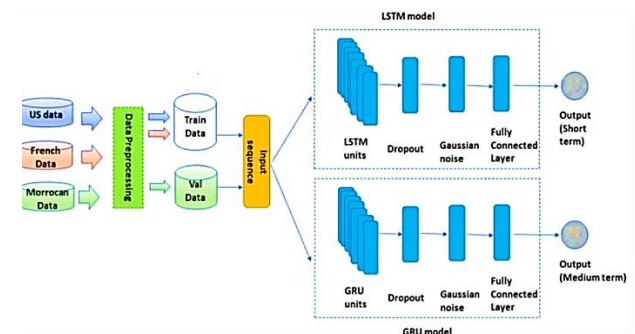


Figure 4: Flow Chart of Methodology

Forget gate layer: Looks at the input data, and the data received from the previously hidden layer, then decides which information LSTM is going to delete from the cell state, using a sigmoid function (One means keeps it, 0 means delete it). It is calculated as:

$$f_t = \sigma(w_f[h_{t-1}, x_t] + b_f) \quad (1)$$

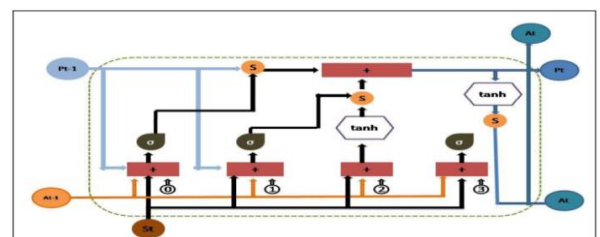


Figure 5: Working of LSTM

Input/Update gate layer: Decides which information LSTM is going to store in the cell state. At first, input gate layer decides which information will be updated using a sigmoid function, then a Tanh layer proposes a new vector to add to the cell state.

VI. CONCLUSION

Healthcare insurance fraud has been depleting medical finances, but conventional, manual fraud detection methods require time and effort. Machine and deep learning methods offer a practical, cost-effective solution that detects healthcare insurance fraud effectively. We built a model that aimed to detect fraud in healthcare claims. This model successfully used logistics regression, random forest, and artificial neural networks to detect fraud with optimal accuracy and good evaluation metrics. Furthermore, each model revealed the significant features causing the outcome. Policy type, education, and age were identified as the most significant features that contributed to fraudulent acts. However, further studies with larger datasets, more variables, and various healthcare providers are advised for better generalization.

REFERENCES

- [1] John T. Hancock, Richard A. Bauder, Huanjing Wang and Taghi M. Khoshgoftaar, "Explainable machine learning models for Medicare fraud detection", *Journal of Big Data*, Springer, pp. 01-31, 2023.
- [2] Eman Nabrawi and Abdullah Alanazi, "Fraud Detection in Healthcare Insurance Claims Using Machine Learning", *MDPI*, pp. 01-11, 2023.
- [3] Mayaki MZA, Riveill M. Multiple inputs neural networks for fraud detection. In: 2022 international conference on machine learning, control, and robotics (MLCR). New York: IEEE; 2022. p. 8–13.
- [4] Salekshahrezaee Z, Leevy JL, Khoshgoftaar TM. A class-imbalanced study with feature extraction via pca and convolutional autoencoder. In: 2022 IEEE 23rd international conference on information reuse and integration for data science (IRI). New York: IEEE; 2022. p. 63–8.
- [5] Sailaja C, Teja GSSK, Mahesh G, Reddy PRS. Detection of fraudulent medicare providers using decision tree and logistic regression models. *J Cardiovasc Dis Res*. 2021;12(3):3343–52.
- [6] Gupta RY, Mudigonda SS, Baruah PK. A comparative study of using various machine learning and deep learningbased fraud detection models for universal health coverage schemes. *Int J Eng Trends Technol*. 2021;69(3):96–102.
- [7] Karmiani, Divit, Ruman Kazi, Ameya Nambisan, Aastha Shah, and Vijaya Kamble. 2019. Comparison of Predictive Algorithms: Backpropagation, SVM, LSTM and Kalman Filter for Stock Market. Paper presented at the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, February 4–6; pp. 228–34.
- [8] Bauder, Richard A., and Taghi Khoshgoftaar. 2018. Medicare fraud detection using random forest with class imbalanced big data. Paper presented at the 2018 IEEE 19th International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, USA, July 6–9; pp. 80–87.
- [9] Chen, Zhen Xing, Lindsey Hohmann, Bidur Banjara, Yi Zhao, Kavon Diggs, and Salisa C. Westrick. 2020. Recommendations to protect patients and health care practices from medicare and medicaid fraud. *Journal of the American Pharmacists Association* 60: e60–e65.
- [10] Herland M, Khoshgoftaar TM, Bauder RA. Big data fraud detection using multiple medicare data sources. *J Big Data*. 2018;5(1):1–21.
- [11] Mackey, Tim Ken, Ken Miyachi, Danny Fung, Samson Qian, and James Short. 2020. Combating health care fraud and abuse: Conceptualization and prototyping study of a blockchain antifraud framework. *Journal of Medical Internet Research* 22: e18623.
- [12] Alharbi, Mohammad F. 2018. An analysis of the Saudi healthcare system's readiness to change in the context of the Saudi National Healthcare Plan in Vision 2030. *International Journal of Health Sciences* 12: 83–87.
- [13] Patel, Pinak, Siddharth Mal, and Yash Mhaske. 2019. A Survey Paper on Fraud Detection and Frequent Pattern Matching in Insurance Claims using Data Mining Techniques. *International Research Journal of Engineering and Technology* 6: 591–94.
- [14] Shamitha, S. Kotekani, and Velchamy Ilango. 2020. A time-efficient model for detecting fraudulent health insurance claims using Artificial neural networks. Paper presented at the 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, July 3–4.
- [15] Suri, Sheffali, and Deepa V. Jose. 2019. Effective Fraud Detection in Healthcare Domain using Popular Classification Modeling Techniques. *International Journal of Innovative Technology and Exploring Engineering* 8: 579–83.