

Deep Learning for Fraud Prediction in Preauthorization for Health Insurance

Aishat Salau, Nwojo Agwu Nnanna, Moussa Mahamat Boukar



Abstract: Health insurance fraud remains a global menace despite the controls implemented to address it; one of such controls is preauthorization. Although, preauthorization promises reduction in fraud, waste and abuse in healthcare, it places undue administrative burden on healthcare service providers and delay in patient care. This limitation has not been thoroughly explored by works of literature in the machine learning domain. In this work, a deep learning model is proposed to learn the preauthorization process for fraud prevention in health insurance for improved process efficacy. In detail, a de-identified HMO preauthorization dataset is used for training the Long Short-Term Memory (LSTM) network. To address class imbalance and avoid data overfitting, the proposed approach utilizes random oversampling and dropout techniques respectively. The experimental results reveal that the proposed model can effectively learn preauthorization request patterns while offering a fraud detection accuracy rate of over 90% with a 2-4% improvement rate in accuracy when compared with previous techniques based on conventional machine learning techniques. The proposed technique is capable of detecting anomalous preauthorization requests based on medical necessity.

Keywords: Deep Learning, Health Insurance Fraud, Machine Learning, Pre-Authorization.

I. INTRODUCTION

According to estimates, healthcare fraud, waste and abuse account for about 10% of total healthcare spending, making it a crucial problem for healthcare systems. [1]. Fraud in health insurance is an intentional provision of false or misleading information to a health insurance company in an attempt to access unauthorized benefits [2]. Although abuse and waste are not particularly related to fraud except when done deliberately, the latter refers to provider practices that fall short of acceptable practices, leading to payment for services that are medically unnecessary, while the former is the unnecessary provision and overuse of healthcare services to get more profit or kickbacks [3]. Fraud can be committed at every level and by all entities involved in the health insurance scheme, which makes it more complex to supervise.

Manuscript received on 11 November 2022 | Revised Manuscript received on 20 November 2022 | Manuscript Accepted on 15 December 2022 | Manuscript published on 30 December 2022.

*Correspondence Author (s)

Aishat Salau*, Student, Department of Computer Science, Nile University of Nigeria, Nigeria E-mail: salauaishat@gmail.com, salauaishat@hotmail.com

Prof. Nwojo Agwu Nnanna, Professor and Head of Department of the Computer Science Department of Nile University of Nigeria, Nigeria

Prof. Moussa, Professor of Computer Science, Departments of Computer Science and Software Engineering, Nile University of Nigeria, Nigeria

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

Most nations' laws describe healthcare fraud as criminal because it drains the government's funds and denies access to beneficiaries who truly need healthcare services. One of the known processes that have been implemented to prevent fraud and abuse is pre-authorization [4]. Pre-authorization is a preventive and procedural measure that necessitates healthcare providers to seek authorization from the HMO before certain services or medications are provided or rendered to patients. It is a method employed by the HMO to keep costs in check by eliminating error, waste, and unnecessary services. This process as shown in Fig. 1 requires medical professionals at the HMO to verify if requested procedures, treatments, or prescriptions are covered in the health plan, medically necessary, or fraudulent. These checks are conducted against clinical guidelines and health plan policies before decisions are made on whether to approve the requests or not. Besides from cost-savings, pre-authorization is also intended to enhance the quality of health care and ensure patients' safety [5]. The contemporary pre-authorization process is time and resource intensive, delays patient care as well as requires a 24/7 presence of several professionals at the HMO to review requests in a timely manner [6]. Considering the large number of requests that have to be reviewed, this process is inherently inefficient and results in errors and poor service delivery. As a result, there is a pressing need for the sector to adopt a more efficient method that will result in significant cost and time savings [7]. With the advancement of technology and the need for increased efficiency, information systems based on data mining and machine learning methods have been employed to automate and simplify this process [8], [9]. Machine learning offers a dynamic approach to fraud detection by offering the system the ability to learn from sample features and improve without being explicitly programmed [10].

Deep learning has attracted a significant amount of interest in recent times. However, its potential in preauthorization has yet to be exploited, especially in the area of predicting fraud waste and abuse in health insurance. In this study, a model based on a deep neural network is proposed to learn the diagnosis-treatment and diagnosis-prescription relationship, which plays a significant role in discovery of medical abuse or fraudulent behavior in preauthorization, as well as determine which requests are medically necessary or otherwise. The result of the experiment shows that the model can improve the discovery rate of fraudulent, non-medically necessary and other abnormal requests from healthcare service providers. In this way, the proposed system is able to support or complement the job of the domain experts for process effectiveness.



II. RELATED WORKS

Not so many works have been carried out in the use of preauthorization for fraud and abuse detection. Araujo proposed a decision support mechanism for the preauthorization process in [11]. To learn this process, Random Tree (RT), Naive Bayes (NB), Support Vector Machine (SVM) and Nearest Neighbour (NN) classifiers were used on a 7-year dental request dataset. The algorithms were evaluated based on the Accuracy (ACC), Precision (P), Recall (R), F-Measure (F1), Area Under the ROC curve (AUC) and Kappa index (K) performance metrics. The best classifiers including SVM, RT and NN were combined to form an ensemble. The selected classifiers performed well individually but performed better as an ensemble, resulting in the accurate classification of about 96% of the prior authorization requests. Araujo also proposed the use of decision tree and induction rules, for the request authorization process in [12], both providing results with ratings above 90%. Also in a bid to improve the learning of the preauthorization process, [4] trained Random Forest, K-Nearest Neighbor (KNN) and SVM models on patients'

historical dataset that were represented using textual features. Precision, recall and kappa are the performance metrics used to evaluate the models. SVM and KNN classifiers reported substantial improvements. Furthermore, in [13], textual features were proposed to further enhance the prior-authorization learning process. Different bag of words techniques were used to extract the textual features and evaluated using Sequential Minimal Optimization, Naive Bayes, J48, Instance based K and Random Forest (RF). The performance of the classifiers was measured using Precision, F1 and Recall with RF giving the best result. Table 1 below presents works of literature on preauthorization for fraud prevention in health insurance based on machine learning techniques, the source and datasets used, the algorithms evaluated and results. The previous works of literature proposed methods based on conventional machine learning algorithms. The data landscape in our modern digital world is changing as data sizes increase. This has necessitated the need to explore deep learning techniques for this purpose as conventional machine learning algorithms offer limited performance in processing and training on voluminous data. [14].

Table- I: Publications on Preauthorization with Machine Learning Methods

Publication	Aim	Methodology	Dataset	Outcome	Limitations
[4]	To learn and improve the preauthorization process based on patients' historical data	Random Forest, KNN and SVM	Brazilian HMO dataset 366 samples	SVM and KNN performed best Refused Class: P = 0.86, R = 1 Approved Class: P = 1, R = 0.98 K = 0.92	Limited data (366 records)
[11]	Support decision-making in prior authorization.	Random Tree, Naive Bayes, Support Vector Machine and Nearest Neighbor	Dental dataset from a non-profit health insurance company. 11,285 samples	Ensemble (SVM, NN, RT) performed best P = 0.96, R = 0.98, ACC = 0.96, F1 = 0.96, AUC = 0.95, K = 0.94	Dental procedures only
[12]	To create a support system for medical reviewers by modeling their behavior	Decision Tree and Induction Rules	Authorization requests from a nonprofit health insurance company Medical data 770,392 samples	Classifier by Induction Rules showed better performance: Authorized Class: R = 97.07%, Unauthorized Class: R = 100%	Classification techniques have fixed point operation, thus hindering analysis using ROC curve.
[13]	Exploring textual features to enhance the prior authorization learning process and evaluation of algorithms	Naive Bayes, Sequential Minimal Optimization, Instance-based K, J48 and Random Forest	Authorization data from a non-disclosed source 3562 samples	RT performed best with Refused Class: P = 0.872, R = 0.826 and F1 = 0.848 Approved Class: P = 0.835, R = 0.878 and F1 = 0.856	Use of textual features that does not take semantics into consideration Limited data 3562 records

III. METHODOLOGY

A. DATASET

In this paper we use real HMO pre-authorization request data for years 2020–2021. The request data contains about 122,000 records, 24 features and is pre-labelled as approved or rejected as deemed fit by the reviewing domain expert based on medical necessity or fraudulent indications. In this section, we describe this dataset in detail. The pre-authorization request data describes the diagnosis and corresponding procedures, treatments or medications as prescribed by the health care provider for the patients. Records within the dataset contain various patient and healthcare provider features, including National Health Insurance Scheme (NHIS) number, patient's first and last name, gender, phone number, address, diagnosis ID and description, treatment ID and description, request communication, primary healthcare provider and ID, referred healthcare provider and ID, request status, approval code and date of approval code. The NHIS number is a unique identification number for health insurance subscribers. In addition, in cases where a preauthorization request is rejected, the corresponding records contain another column

that describes the reason for rejection. The dataset contains both numerical and categorical values. An example of the preauthorization dataset is presented in Table 2.

However, due to privacy, ethical and legal reasons, the dataset was de-identified in compliance with the HIPAA regulation, by taking out personal identifiable information (PII), such as unique IDs, dates of birth, phone numbers and addresses from the dataset. In addition, fake IDs were generated to substitute real IDs in the dataset to identify all subjects anonymously. Consequently, the dataset was pre-processed to enhance the data quality and reduce the amount of irrelevant information.

B. Data Preprocessing

Data preprocessing helps in the creation of standardized dataset suitable for model training. This process is posed with several challenges due to the heterogeneity, inconsistencies and prevalence of missing values in healthcare data. These missing values may affect data analysis and accuracy of the model [15].

This was handled by enumerating records with missing values and then substituting with appropriate imputations depending on the data missing.

In health insurance, there are no general factors that can be used to determine fraud or tell if a procedure is medically necessary or not, due to the multivariate nature of healthcare data. This was one of our major challenges; to determine the factors that have significant impact on deciding whether requests are medically necessary for detection of fraudulent requests present in the dataset. With the help of a domain expert, features that were not necessary for decision making at the time of preauthorization were eliminated, leaving required attributes. Since, the major concern is identifying fraud and abuse by establishing the medical necessity of requests, the provider-level attributes like healthcare providers' names and IDs were removed from the dataset as they are not relevant to decision making. Only 7 features remained in the dataset after a total of 12 characteristics were dropped. The resulting feature set and associated data types are outlined in Table- II.

Table- II: Feature Set and Corresponding Data Type

Features	Datatype
Age	Numerical
Gender	Categorical
Diagnosis_ID	Categorical
Treatment_ID	Categorical
Request_Communication	Categorical
Request_Status	Categorical

All categorical features must be properly encoded before they can be processed by a neural network. Basically, one-hot coding can be used to vectorise categorical variables; however, it drastically increases dimensionality of the dataset and does not capture the semantic relationships between words [16]. Hence, in this work we utilise word embedding to vectorise categorical features. After these data processing steps are completed, the resulting dataset had 117343 samples and exhibits the challenge of class imbalance. Class imbalance occurs when there are significantly more instances of one class (the majority class) than there are of another class (minority class) [17]. This phenomenon is considered as one of the major problems in data mining and it is mainly encountered in situations where anomaly detection is crucial [18], [19] as in the case under consideration. The number of authorised samples (117068) is exceedingly greater than the number of rejected samples (275). Fig 1. presents the disparate levels of data before employing a resampling method. can be seen in Fig 1. while class levels after ROS implementation is illustrated in Fig 2.

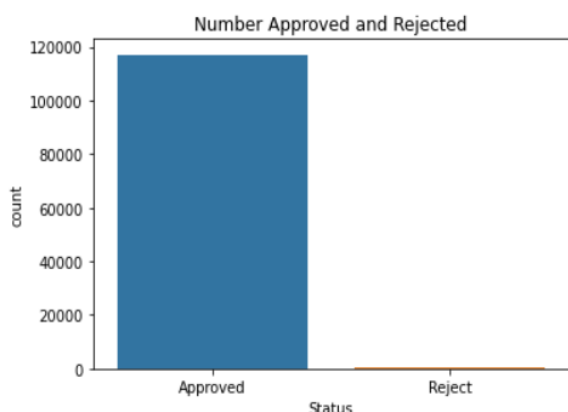


Fig. 1. Imbalance Data Levels before Resampling

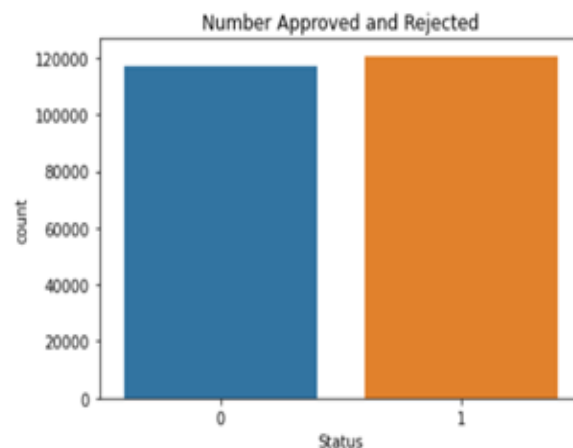


Fig. 2. Data Level after ROS showing the Number of Positive and Negative Samples

The majority of machine learning algorithms have difficulty in building models that accurately classifies samples in the minority class, as a result of bias towards the majority class samples due to its increased occurrence in the dataset [20]. Thus, data-level class balancing method using random over-sampling (ROS) was explored to address this challenge. The ROS approach entails duplicating minority class samples until the appropriate amount of class balance is attained, and is best suited for neural networks [21]. Since there are many more normal requests than there are anomalous requests, the rare class must be over-sampled at high rates in order to even out the class distributions. However, if under-sampling is employed until class balance is achieved, we run at a risk of losing data samples, because with this technique, samples from the majority group are randomly removed until all classes are the same size [21]. This can be disadvantageous with deep learning, performance of the a deep learning model decreases with a decrease in data. The most efficient strategy to enhance performance on the test set is to use more training data [22]. Result Subsequently, the dataset was split 80:20. 80% of the data was used for training the neural network while the remaining 20% was used for model validation.

C. MODEL

Based on the limitations of the previous works, this work will employ the use of textual features and deep neural networks to learn preauthorization request patterns for fraud prevention in health insurance. The Long Short Term Memory (LSTM), a class of Recurrent Neural Network (RNN) is explored to learn the diagnosis-treatment and diagnosis-prescription relationship, which plays a significant role in the discovery of medical abuse or fraudulent behavior in preauthorization. LSTM addresses the vanishing gradient issue present in conventional RNN by substituting the self-connected hidden units with memory blocks. They give the learning network the ability to store data for longer periods as well as select when to acquire new information and when to dispose of previously learned data. [23].



Deep Learning for Fraud Prediction in Preauthorization for Health Insurance

This is desirable for the fraud detection problem as health insurance policies and fraud patterns are known to be dynamic and evolve overtime. Furthermore, as categorical features need to be converted to vectors that can be fed into the neural network, the default Keras embedding layer is employed for word embedding. To optimize the model, the Adam optimizer was employed as research has demonstrated that it performs better than other well-known optimizers [24]. All hidden layer neurons utilize the rectified linear unit (ReLU) activation function, and the output layer neurons employ the sigmoid activation function to calculate posterior

probabilities. It has been demonstrated that the ReLU activation function alleviates the vanishing gradient issue and speeds up training. [25]. A dropout layer is also used before the output layer, to reduce overfitting and improve generalization of the model to new data by randomly deactivating non-output neurons during each iteration and forcing the model to learn more robust features. [26], [27]. Fig. 3. and Fig. 4. illustrate the process flow and proposed architecture for the LSTM model used in this work for classifying the pre-authorization requests.

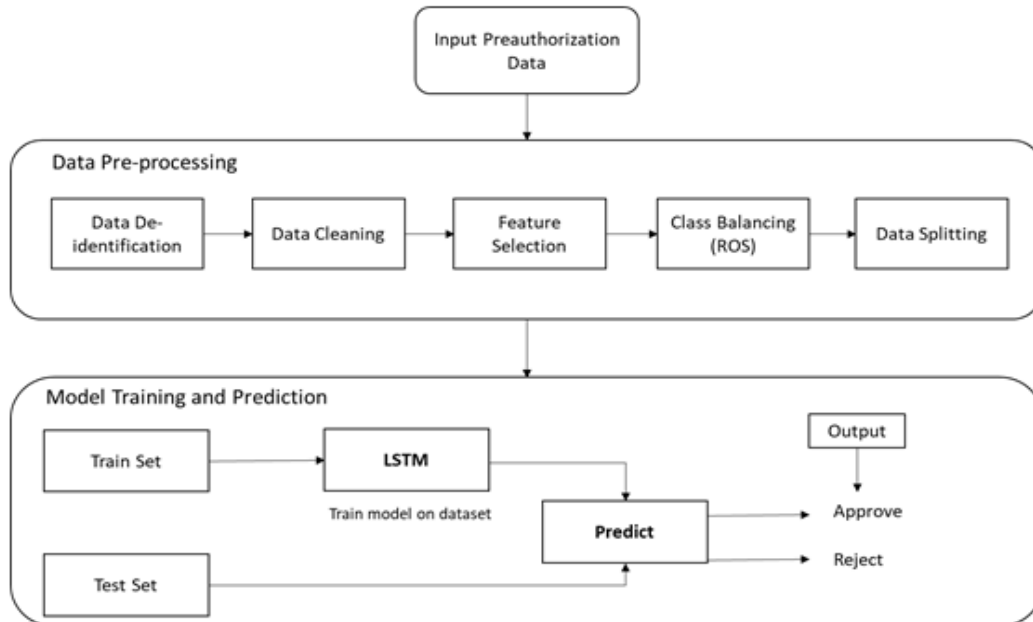


Fig. 3. Process Flow for Proposed Deep Learning Framework for Pre-authorization

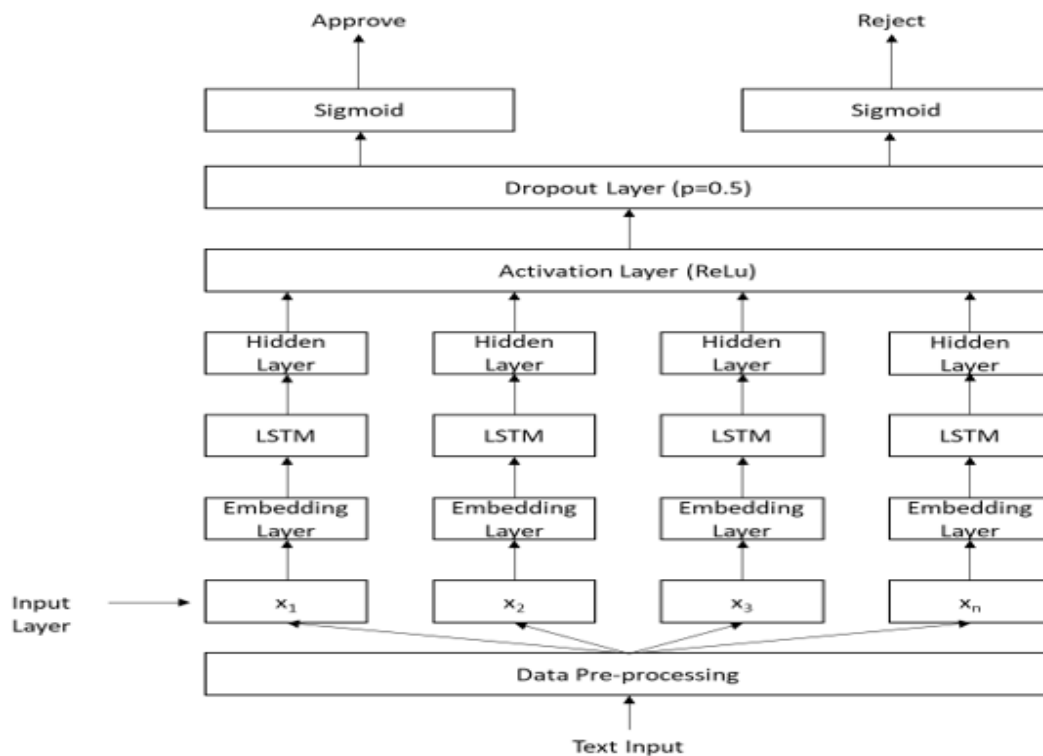


Fig. 4. Proposed LSTM Architecture for Pre-authorization

D. Performance Metrics

This study employs a number of complementary evaluation metrics to provide a clear picture of model performance. The confusion matrix, accuracy, precision, recall and F1 score are reported in this study. Since this is a binary classification problem, there are only 2 classes; the positive and negative, there are 4 possible outputs on the confusion matrix, the True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN). A positive sample that is classified as positive is a TP, if classified as negative is considered as FN. A negative sample classified as negative is considered as TN, if classified as positive is considered a FP. The metrics used are dependent on these values. The accuracy as in (1) is a measure of how close the predicted value is to the true value, precision (2), measures the positive samples that are correctly predicted to be positive, while recall (3) is a measure of the negative group that are correctly predicted to be negative. The F1-score (4) reports the harmonic mean of precision and recall, which ranges between 0 and 1. A large F-score represents high classifier efficacy. The confusion matrix shows a comparison of predicted labels to true labels.

$$accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{1}$$

$$precision = \frac{TP}{TP + FP} \tag{2}$$

$$recall = \frac{TN}{TN + FN} \tag{3}$$

$$F1 - Score = 2 * \frac{precision * recall}{precision + recall} \tag{4}$$

IV. RESULT AND DISCUSSION

The capability of the LSTM network to predict fraud, waste and abuse in preauthorization request is expressed as a binary classification problem. The confusion matrix is used to visualize the LSTM classifier's prediction rate as illustrated in Fig. 5. We can read therefrom that the LSTM model predicts the fraudulent and normal requests with an accuracy of 99.4%. The number of samples that were misclassified for the normal and anomalous requests are 239 and 0 respectively (0.05% and 0%).

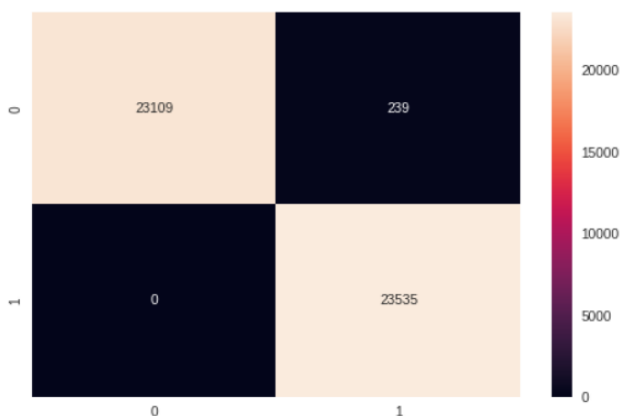


Fig. 5. Confusion Matrix of the LSTM Binary Classifier showing the Correct Predictions in the Cream Diagonals and Incorrect Predictions on the Black Diagonals.

A model has an accuracy of 99%, depicts excellent model performance. However, accuracy is susceptible to class imbalance; two classifiers with same accuracy may perform differently in terms of the predictions they each produce [28]. Hence, the precision, recall and F1-score, which indicates the true positive rate and true negative rate, are calculated to find the actual positive samples and actual negative samples. Therefore, although the model achieved high accuracy, the precision, recall and F1-score will be considered significant to evaluation of the prediction correctness of the model. Table- III presents the performance metrics of the classifier for before and after data resampling with ROS. The accuracy, precision, recall and F1 score of the model is presented for both experiments.

Table- III: Result of LSTM Model Evaluation

Metrics	Before ROS	After ROS
Accuracy	99.8%	99.4%
Precision	0.69	0.98
Recall	0.17	1.00
F1-Score	0.28	0.99

According to the experiment, the proposed LSTM model is capable of detecting anomalous preauthorization requests by learning to make decisions for preauthorization requests based on medical necessity. Using the diagnosis and treatment IDs, the model is able to accept or reject requests on the basis of learned diagnosis-treatment and diagnosis-treatment relationships.

V. CONCLUSION

Fraud cases in the healthcare system have been on the increase in recent years and patients who genuinely need medical care suffer because of the unavailability of services resulting from lack of funds caused by fraud. Fraud and abuse can be deterred through preauthorization. However, the process is time consuming and can be inefficient with an increase in request. Regrettably, just a few works have been done in this area. This research work has explored the use of deep learning to learn the state of art machine learning methods for combatting fraud in the health insurance system through preauthorization.

This paper has presented a LSTM network for fraud, waste and abuse detection through preauthorization. Four major performance metrics are used to evaluate the performance of the LSTM classifier, and the findings demonstrate that the suggested strategy outperforms the state-of-the-art techniques that used conventional machine learning methods.

By eliminating class imbalance from the dataset using the ROS method, high precision, recall and F1-scores were achieved. We conclude that deep learning with ROS gives a better result when compared with previous traditional method used to learn the pre-authorization method as seen in reviewed literature. In this study, the size of the dataset is quite limited, due to the non-availability of labelled data samples and difficulty in collection of healthcare dataset due to its sensitivity.



It is therefore anticipated that the training dataset might not cover every possible diagnosis-treatment case. Similarly, it is essential for fraud detection techniques to be capable of adapting to constantly changing fraudulent behaviors. Hence, further work in this area should consider implementation of semi supervised learning methods e.g. active learning to give room for progressive labelling and model training and update [29]. Furthermore, unlike health insurance claims data, there are currently no publicly available preauthorization datasets. This is also attributed to privacy concerns which often prevents the publication of such data. As a result, researchers are compelled to develop their own models with personally sought data or data they have independently collected, and it is difficult to compare results when each research uses a different dataset. Finally, advanced deep learning and class balancing methods can also be explored for better performance.

REFERENCES

- J. Li, Q. Lan, E. Zhu, Y. Xu, and D. Zhu, "A Study of Health Insurance Fraud in China and Recommendations for Fraud Detection and Prevention," *J. Organ. End User Comput.*, vol. 34, no. 4, pp. 1–19, Jul. 2022, doi: 10.4018/JOEUC.301271. [CrossRef]
- W. L. Shiau, K. Siau, Y. Yu, and J. Guo, "Research Commentary on IS/IT Role in Emergency and Pandemic Management: Current and Future Research," <https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/JDM.2021040105>, vol. 32, no. 2, pp. 67–75, Jan. 2021, doi: 10.4018/JDM.2021040105. [CrossRef]
- J. Bush, L. Sandridge, C. Treadway, K. Vance, and A. C. D. Ph, "Medicare fraud, waste and abuse," undefined. 2017.
- K. Farias, P. Santos Neto, A. Santana, and R. Bezerra Neto, "Using historical information of patients for prior authorization learning," in *Proceedings - 2019 Brazilian Conference on Intelligent Systems, BRACIS 2019*, Oct. 2019, pp. 598–603, doi: 10.1109/BRACIS.2019.00110. [CrossRef]
- "Considerations for Improving Prior Authorization in Healthcare," 2019.
- A. Medical Association, "2019 AMA prior authorization (PA) physician survey," 2019.
- Caqh, "2018 CAQH INDEX ® A Report of Healthcare Industry Adoption of Electronic Business Transactions and Cost Savings," doi: 10.1001/jama.2018.1150. [CrossRef]
- N. Ghuse, P. Pawar, and A. Potgantwar, "An Improved Approach For Fraud Detection In Health Insurance Using Data Mining Techniques," 2017, Accessed: Apr. 17, 2020. [Online]. Available: www.ijrnsnc.org/Availableonlineatwww.ijrnsnc.org.
- T. S. Yange, "A Fraud Detection System for Health Insurance in Nigeria," *J. Heal. Informatics Africa*, vol. 6, no. 2, pp. 64–73, 2019, doi: 10.12856/JHIA-2019-V6-I2-256.
- C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning," *Electron. Mark.*, vol. 31, no. 3, pp. 685–695, Sep. 2021, doi: 10.1007/S12525-021-00475-2/TABLES/2. [CrossRef]
- F. H. D. Araújo, A. M. Santana, and P. de A. Santos Neto, "Using machine learning to support healthcare professionals in making preauthorisation decisions," *Int. J. Med. Inform.*, vol. 94, pp. 1–7, Oct. 2016, doi: 10.1016/j.ijmedinf.2016.06.007. [CrossRef]
- F. Araújo, L. Moraes, A. Santana, P. S. Neto, P. Adeodato, and É. Leão, "Evaluation of the use of computational intelligence techniques in medical claim processes of a health insurance company," in *Proceedings of CBMS 2013 - 26th IEEE International Symposium on Computer-Based Medical Systems*, 2013, pp. 23–28, doi: 10.1109/CBMS.2013.6627759. [CrossRef]
- G. V. M. Junior, J. P. A. Vieira, R. L. De Sales Santos, J. L. N. Barbosa, P. De Alcantara Dos Santos Neto, and R. S. Moura, "A study of the influence of textual features in learning medical prior authorization," in *Proceedings - IEEE Symposium on Computer-Based Medical Systems*, Jun. 2019, vol. 2019-June, pp. 56–61, doi: 10.1109/CBMS.2019.00021. [CrossRef]
- M. Gheisari, G. Wang, and M. Z. A. Bhuiyan, "A Survey on Deep Learning in Big Data," *Proc. - 2017 IEEE Int. Conf. Comput. Sci. Eng. IEEE/IFIP Int. Conf. Embed. Ubiquitous Comput. CSE EUC 2017*, vol. 2, pp. 173–180, Aug. 2017, doi: 10.1109/CSE-EUC.2017.215. [CrossRef]
- E. Ammar, M. A.-S. Saleh, A. Firas, and S. Walid, "ILA4: Overcoming missing values in machine learning datasets – An inductive learning approach," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. Volume 34, no. Issue 7, pp. 4284–4295, doi: <https://doi.org/10.1016/j.jksuci.2021.02.011>. [CrossRef]
- F. K. Khattak, S. Jeblee, C. Pou-Prom, M. Abdalla, C. Meaney, and F. Rudzicz, "A survey of word embeddings for clinical text," *J. Biomed. Inform.*, vol. 100, p. 100057, Jan. 2019, doi: 10.1016/j.YJBINX.2019.100057. [CrossRef]
- V. López, A. Fernández, and F. Herrera, "On the importance of the validation technique for classification with imbalanced datasets: Addressing covariate shift when data is skewed," 2014, doi: 10.1016/j.ins.2013.09.038. [CrossRef]
- Y. Qiang and W. Xindong, "10 Challenging problems in data mining research," *Int. J. Inf. Technol. Decis. Mak.*, vol. 5, no. 4, pp. 597–604, 2006, doi: 10.1142/S0219622006002258. [CrossRef]
- S. Rodda and U. S. R. Erothi, "Class imbalance problem in the Network Intrusion Detection Systems," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Mar. 2016, pp. 2685–2688, doi: 10.1109/ICEEOT.2016.7755181. [CrossRef]
- M. R. Parsaei, S. M. Rostami, and R. Javidan, "A Hybrid Data Mining Approach for Intrusion Detection on Imbalanced NSL-KDD Dataset," 2016. Accessed: May 27, 2019. [Online]. Available: www.ijacsa.thesai.org.
- M. Buda, A. Maki, and M. A. Mazurowski, "A systematic study of the class imbalance problem in convolutional neural networks," *Neural Networks*, vol. 106, pp. 249–259, Oct. 2018, doi: 10.1016/J.NEUNET.2018.07.011. [CrossRef]
- I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. 2016.
- A. Sherstinsky, "Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network," *Phys. D Nonlinear Phenom.*, vol. 404, p. 132306, Mar. 2020, doi: 10.1016/J.PHYSD.2019.132306. [CrossRef]
- M. Yaqub et al., "State-of-the-Art CNN Optimizer for Brain Tumor Segmentation in Magnetic Resonance Images," *Brain Sci.* 2020, Vol. 10, Page 427, vol. 10, no. 7, p. 427, Jul. 2020, doi: 10.3390/BRAINSCI10070427. [CrossRef]
- M. M. Noel, A. L. A. Trivedi, and P. Dutta, "Growing Cosine Unit: A Novel Oscillatory Activation Function That Can Speedup Training and Reduce Parameters in Convolutional Neural Networks," Aug. 2021, doi: 10.48550/arxiv.2108.12943.
- N. Srivastava, G. Hinton, ... A. K.-T. journal of machine, and undefined 2014, "Dropout: a simple way to prevent neural networks from overfitting," *jmlr.org*, vol. 15, pp. 1929–1958, 2014, Accessed: Nov. 06, 2022. [Online]. Available: https://www.jmlr.org/papers/volume15/srivastava14a/srivastava14a.pdf?utm_content=buffer79b43&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.
- S. Hahn and H. Choi, "Understanding dropout as an optimization trick," *Neurocomputing*, vol. 398, pp. 64–70, Jul. 2020, doi: 10.1016/J.NEUCOM.2020.02.067. [CrossRef]
- A. Tharwat, "Classification assessment methods," *Appl. Comput. Informatics*, vol. 17, no. 1, pp. 168–192, 2020, doi: 10.1016/J.ACI.2018.08.003/FULL/PDF. [CrossRef]
- P. Kumar and A. Gupta, "Active Learning Query Strategies for Classification, Regression, and Clustering: A Survey," *J. Comput. Sci. Technol.* 2020 354, vol. 35, no. 4, pp. 913–945, Jul. 2020, doi: 10.1007/S11390-020-9487-4. [CrossRef]

AUTHORS PROFILE



Aishat Salau, is a student of the Department of Computer Science at Nile University of Nigeria, she holds a Masters of Science degree in Information Security from Royal Holloway University of London, England and a Bachelor of Technology degree in Computer Engineering from Ladoko Akintola University of Technology, Ogbomosho, Nigeria. She's an Information Technology and cybersecurity professional with over five years' experience and has contributed in different capacities to the nation's cybersecurity resilience. She is also interested in improving the use of information technology in the healthcare industry. Her research interests include Deep Learning, Machine Learning, Data Analytics, Health Informatics and Cybersecurity.





Prof. Nwojo Agwu Nnanna is a Professor and Head of Department of the Computer Science Department of Nile University of Nigeria. Dr. Nnanna received his PhD degree from Texas Tech University, Lubbock Texas, United States of America in 1996. He has taught Computer Science and Mathematics at both undergraduate and graduate levels in the United States and Nigeria. His research interests are in the

areas of artificial intelligence, design of robust optimization models for machine learning algorithms, robotics, dynamical systems, numerical computation, and systems and control theory. He has written a number of peer-reviewed journal articles in numerical computation and systems and control theory, application of semi-Lagrangian integration techniques to Navier-Stokes equations, etc.



Prof. Moussa is a Professor of Computer Science in the Departments of Computer Science and Software Engineering at Nile University of Nigeria, where he has been a faculty member since 2013. He is the Dean of the Faculty of Natural and Applied Sciences. He completed his PhD and M.Sc. at Blacksea University, Georgia and International Alatau University, Kyrgyzstan, respectively. His

research interests lie in the areas of Programming Languages, Machine Learning and Content Management System Technology (CMS). He has collaborated actively with researchers in several other disciplines of Computer Science, particularly Computer Programming on problems at the software interface and Machine Learning.