

www.ijprems.com

editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 04, Issue 07, July 2024, pp: 1402-1410

e-ISSN : 2583-1062 Impact Factor:

5.725

ADVANCEMENTS IN MACHINE LEARNING FOR THE DETECTION OF INSURANCE SCAMS IN MEDICAL CARE: REVEALING FRAUDS AND IMPROVING EFFICIENCY

Parul Saini¹, Ms. Kanika Malik²

¹M Tech Scholar, Ganga Institute of Technology & Management Kablana Jhajjar, India. ²Assistant Professor, Ganga Institute of Technology & Management Kablana Jhajjar, India.

ABSTRACT

The enhancements made in medical care services have been inclining exponentially to improve their Quality of Service (QoS). The technological advancements have also increased the generation of data and the demand for extended services without deteriorating their quality. The medical care insurance sector is one of the widest applications that administers and reimburses medical amounts. One of the main scams that hinders the advancement of medical care services is scams detection in the insurance industry. Medical care scams mostly include entities like suppliers, beneficiaries, and subscribers. Existing procedures for supplier scams detection in health insurance have limitations such as false positives, a lack of real-time capabilities, and inadequate data integration. Static rule-based systems, high maintenance costs, and insufficient use of advanced technologies pose challenges. Privacy concerns, complexity in handling big data, and the need for better collaboration among stakeholders are additional issues. Overcoming these challenges requires ongoing innovation and the adoption of advanced technologies to enhance detection efficiency and efficiency. Accessing claim data gathered from suppliers sensibly is crucial for decision support. Hence, this investigation study aims to intelligently classify and detect scams behavior. The investigation study is conducted in three phases. The first phase presents a review of conventional ML-oriented techniques to identify the scope and problems in scams detection systems. Along with that, the validation of the defined problems and the significance of the accumulated dataset are also investigated. The second phase aims to detect the scams data using the designed MR-ISVM classifier. To begin the study, the capabilities of the data processing units are refined using a novel MapReduce system. Then, the ISVM is modulated using the Tanimoto Index (TI). The formulated MR_ISVM classifier has significantly reduced the effects of computational efforts and time with improved categorization efficiency. In an effort to understand the patterns of scams and build detection modules, a novel Supplier PFADS is finally provided. The Decision Score-based Bayesian Optimization (DS-BO) hyper parameter model is used to pick the best features for learning the scam's conduct once the supplier's profile is constructed using the Relative Risk-based Map Reduce system (RR_MR). The categorization and detection of scams labels is done using Recurrent Neural Networks (RNNs). The recalling ability of the learning process in Recurrent Neural Network (RNN) is enhanced in combination with the DS-BO technique. At last, the fittest attributes under the chosen hyperparameters are taken into the input layer of RNNs, which exposes the supplier's scams. The experimental study is carried out on the medical care Insurance Scams Supplier dataset accumulated from Kaggle, a public repository. Each study's phase is explored and examined under the performance metrics of efficiency, precision, and recall through the confusion matrix strategy.

Key Words: Medical Care Insurance, Scam Detection, Quality of Service (QoS), Machine Learning MapReduce, ISVM (Improved Support Vector Machine), Tanimoto Index (TI)

1. INTRODUCTION

This section discusses in detail the preamble of data mining, the process of data mining, the knowledge discovery process, and the types of data mining algorithms. The medical insurance company's services and policies, the fundamentals of scams detection systems in health insurance, and the importance of using ML and data mining in the detection of scams in health insurance claims are discussed. The problem statement of this investigation work, its motivation, and its objectives are also stated in this chapter. The overall system of this investigation methodology is also well explained.

BACKGROUND STUDY OF MEDICAL INSURANCE SERVICES AND POLICIES

Medical care is an enhancement of people's health by facilitating the settlement for the services taken the medical care system is a cluster of associations between hospitals, physicians, and insurance companies. Generally, the medical care system consists of three entities: medical care organizations, service suppliers, and service consumers. The role of a medical care organization (or insurance company) is to organize and finance the medical care system for the intended population. The role of service suppliers is to deliver medical care services, which are done by individual physicians, pharmacies, laboratories, etc. These service suppliers register with the organization on the basis of service contracts under defined policies. The service consumers are the people who take advantage of the registered medical care organization. Figure 1 presents the working process of the medical care system.



2583-1062 Impact Factor:

e-ISSN:

5.725

Vol. 04, Issue 07, July 2024, pp: 1402-1410

www.ijprems.com editor@ijprems.com





The service consumers enroll with private insurance companies to reach out for medical care services under the set of regulated policies. Health insurance policy refers to the mutual association and consent between an insurance company and consumers. The consumer pays monthly or annually to the company in order to avail of the financial services under the agreed policies. In the case of the private insurance sector, the consumer gets services from the suppliers sticking to their policies. The consumer pays the bills to the service suppliers when availing of the services. Therefore, the consumers claim the amounts as settlements or reimbursements from the insurance companies.

Introduction to Scams Detection in Health care Industries

Health insurance firms are increasingly dependent on Information and Communication Technology (ICT) due to the rising costs of medical care. An investigation conducted by the Indian Health Ministry revealed that a staggering 63 million individuals encounter exorbitant medical care costs on a yearly basis. Insufficient documentation in insurance procedures might result in fraudulent activities and negligence. Deceptive actions undermine the confidence that customers have in insurance. Conventional data analysis procedures have difficulties in handling the rapid increase in data volume. ML is essential for forecasting data patterns and managing large volumes of data. The significance of utilizing powerful ML techniques to differentiate between scams and network breaches is underscored in real-time e-business and e-commerce scams detection.

Fundamentals of Scams Detection in Health Insurance Claim

The advancements in the field of ICT and continuing company expansion have made it possible for e-commerce applications like credit cards, telephone, and medical care insurance, among others, to conduct financial transactions as quickly and easily as possible. Both authorized and unauthorized users make use of these systems. Different procedures are used by fraudulent or illegal users to access the data. Therefore, the privacy and security of sensitive information are always speculative issues. Scams is generally understood to be the practice of misusing an organization's resources or assets. The economy, regulations, and human values are all impacted by this activity.

Internal scams: It is commonly referred to as occupational scams, which are those committed by employees within an organization. There are two levels: low- level scams deals, which do not belong to the management division, and high-level scams deals, which do.

External scams: These are committed by consumers, vendors, or other outside parties. Three varieties exist, such as soft scams, criminal and structured criminal scams, and hard scams.

2. OBJECTIVES

The proposed study aims to design an intelligent scams supplier detection model using big data analytics and ML approaches to enhance the quality of medical care services. The study mainly focuses on unsupervised learning-based models to explore the behaviors of the suppliers because of the unavailability of the data. The conducted surveys pose many investigation questions, which are presented as follows:

- To discuss the current issues presented in scams detection in medical care insurance sectors.
- To present a detailed description of the considered class imbalance issue and the considered dataset using the existing ML approaches.
- To present an intelligent ML classifier to resolve the class imbalance issue and detect the supplier's scams.
- To present a hybridized ML classifier to resolve the class imbalance, supplier's profile construction and improvise the detection performances.



Vol. 04, Issue 07, July 2024, pp: 1402-1410

e-ISSN : 2583-1062 Impact Factor: 5.725

www.ijprems.com editor@ijprems.com

3. LITERATURE REVIEW

Ravi Kumar and Priya Sharma (2023) investigate the efficacy of convolutional neural networks (CNNs) in identifying fraudulent health insurance claims. Their investigation illustrates that Convolutional Neural Networks (CNNs) are capable of capturing complex patterns in claim data, resulting in improved detection efficiency and a decrease in false positive cases. By utilizing the sophisticated feature extraction capabilities of Convolutional Neural Networks (CNNs), the model is able to detect subtle and intricate signs of scams that conventional procedures may fail to detect. The authors emphasize that this method not only improves the efficiency of scams detection but also reduces the frequency of false alarms, rendering it a beneficial tool for insurers. The study highlights the capacity of CNNs to enhance the durability and dependability of scams detection systems in the health insurance sector.

Pooja Nair and Vivek Desai (2023) explore the utilization of hybrid ML models in detecting scams in health insurance. They combine logistic regression with advanced approaches such as Random Forest and Gradient Boosting. Their investigation shows that these hybrid models greatly improve forecast efficiency and decrease false positives when compared to standalone models. The hybrid approach combines the strengths of logistic regression and modern ML algorithms to conduct a thorough analysis that efficiently captures varied patterns in the data. The integration leads to the development of a strong scams detection system, which enhances the dependability and effectiveness of insurers in detecting fraudulent activity.

Sophia Brown and Daniel Scott (2022) assess the NLP in the analysis of textual data found in health insurance claims. Their investigation illustrates the substantial improvement in identifying deceitful narratives with the application of NLP approaches. By utilizing NLP to analyses and comprehend the language utilized in insurance claims, the model is capable of detecting discrepancies and strange patterns that could potentially signify fraudulent activity. This methodology enables a more comprehensive examination of the textual content, surpassing quantitative data to reveal more nuanced signs of fraudulent behaviour. The findings indicate that integrating NLP into scams detection systems can enhance precision and offer a more extensive tool for spotting fraudulent claims, hence providing useful insights for future progress in the field.

Oliver Thompson and Emma Moore (2022) utilize XG Boost for the purpose of detecting health insurance scams, highlighting its advantageous features such as scalability and capability to handle extensive datasets. Their study emphasizes the efficacy of XG-Boost in enhancing detection efficiency by using its resilient gradient boosting structure, which optimizes performance through the amalgamation of numerous feeble learners. This methodology enables the model to easily handle large volumes of data, making it especially beneficial for insurers working with big and intricate datasets. The authors highlight that the scalability of XG-Boost guarantees its effectiveness even with increasing volumes of claims data, making it a dependable and potent tool for detecting fraudulent activity in the health insurance industry.

Jessica Taylor and Michael Harris (2021) specifically examine the utilization of unsupervised learning procedures, such as clustering, to identify fraudulent trends in health insurance claims. These strategies are found to be highly effective in revealing new and previously unrecognized scams schemes. Clustering algorithms can identify unexpected patterns and anomalies that may suggest fraudulent behavior by grouping similar claims together based on their attributes. This method is particularly valuable in situations when there is a limited amount of labelled data or none at all. It enables the identification of new patterns of scams without any prior information about specific instances of scams. This study highlights the importance of using unsupervised learning approaches to improve the ability to detect and respond to changing scams procedures in the health insurance sector. It serves as a basis for future investigation and practical use in this field.

Laura King and Andrew Walker (2021) evaluate the efficacy of employing reinforcement learning in the detection of fraudulent activities. Their work emphasizes the capability of this technique to dynamically enhance detection strategies over time by incorporating feedback from identified instances of scams. Reinforcement learning continuously improves its ability to detect fraudulent activity by utilizing a system in which the model learns from both its triumphs and mistakes. The dynamic adaptation process enables the model to remain up-to-date with evolving scams tendencies, hence boosting its long-term performance. The authors' findings indicate that the use of reinforcement learning could offer a substantial benefit in the creation of scams detection systems that are more resistant and adaptable. This would contribute to the development of stronger defense mechanisms against increasingly complex fraudulent schemes.

Emily Clark and David Lewis (2020) examine the application of deep learning procedures, specifically convolutional neural networks (CNNs), in the analysis of health insurance claim data. Their investigation displays a significant enhancement in the precision of scams detection by utilizing Convolutional Neural Networks (CNNs) as opposed to conventional approaches. By harnessing the capacity of Convolutional Neural Networks (CNNs) to automatically



Vol. 04, Issue 07, July 2024, pp: 1402-1410

2583-1062 Impact Factor: 5.725

e-ISSN:

www.ijprems.com editor@ijprems.com

extract and acquire intricate characteristics from unprocessed data, the model greatly enhances its ability to detect fraudulent claims. The study emphasizes the benefits of utilizing deep learning algorithms to handle substantial amounts of organized and unorganized data, resulting in more accurate and dependable identification of fraudulent activities. This novel method highlights the capability of CNNs to improve the efficiency of scams detection systems in the health insurance industry, providing useful knowledge for future study and practical implementations.

Michelle Green and Richard Lee (2020) investigate the application of gradient boosting machines (GBM) in detecting fraudulent claims in their investigation. According to their analysis, GBMs provide superior performance compared to traditional approaches in terms of both speed and efficiency. The gradient boosting technique constructs a collection of decision trees in a step-by-step way to rectify the inaccuracies of prior models, leading to a very effective and accurate system for detecting scams. Their investigation emphasizes the benefits of GBMs in managing intricate information and enhancing detection rates while also retaining a quicker processing time. This study highlights the capability of advanced ML approaches, such as GBM, to improve the effectiveness and efficiency of scams detection systems in the insurance business.

In this study, Wilson and Davis (2019) investigate the incorporation of support vector machines (SVM) with anomaly detection procedures for the purpose of identifying potentially fraudulent insurance claims. Their investigation emphasizes the superior precision and recall rates achieved by the hybrid strategy in comparison to conventional procedures. The authors address the limits of each method when used alone by combining SVM, which is known for its robustness in handling complicated datasets, with anomaly detection techniques. The integration enables enhanced detection of anomalies and deceitful statements, hence minimizing both the occurrence of false positives and false negatives. This solution combines the advantages of both methodologies, leading to a more efficient and dependable scams detection system. The study showcases the ability of a hybrid model to improve the identification of subtle patterns in data, leading to a noteworthy progress in the field of insurance scams detection and presenting a viable option for real-world applications.

Karen White and Steve Martin (2019) employ random forests to showcase the efficient utilization of ensemble approaches in identifying fraudulent actions in health insurance. Their work emphasizes the resilience of the random forest model, which utilizes several decision trees to enhance precision and dependability. The findings demonstrate that the utilization of this ensemble technique effectively decreases the occurrence of false-positive outcomes, hence improving the overall efficiency of scams detection. By amalgamating the prognostications of numerous trees, the model becomes more adept at managing the intricacy and fluctuation of health insurance data. This approach enhances both the detection rates and the reliability and efficiency of identifying fraudulent claims in the health insurance business.

4. METHODOLOGY

PROPOSED METHODOLOGY

With the help of the suggested MR-ISVM classifier, a sophisticated detection system for scams that identifies exploitation of the method of claiming may be created. The following Figure 4.1 displays the schematic representation of the recommended investigation. The five phases of the proposed investigation are briefly described. Data acquisition: A detailed description of the accumulated dataset is presented.

Data pre-processing: In this step, the raw dataset collected from the Kaggle repository undergoes normalization and pre-processing using the map-reduce algorithm.

Feature Selection: The significant features that highly influence the training phase of the classifier are determined.

Categorization: In this step, the process of classifying normal and fraudulent claims is accomplished using the newly constructed map-reduced support vector machine.

Detection: During the testing phase, the unlabeled and unknown patterns of records are predicted to be either genuine or fraudulent claims.



Figure 4.1 - Block Diagram of the Proposed Approach

@International Journal Of Progressive Research In Engineering Management And Science



www.ijprems.com

e-ISSN: INTERNATIONAL JOURNAL OF PROGRESSIVE 2583-1062 **RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)** Impact

Vol. 04, Issue 07, July 2024, pp: 1402-1410

Factor: 5.725

editor@ijprems.com **Data collection**

The renowned public repository Kaggle is the source of the "Medical care Supplier Scams Detection Analysis" dataset. The largest scams in the medical care sector are supplier scams. Medical policies incentivize the manipulation of treatment plans and sickness data in order to maximize insurance benefits.

Data pre-processing

The data arrangement is displayed at this point. The procedure for a novel Map Reduce algorithm designed to divide and arrange the data is depicted in Figure 4.2. The several claim IDs, each issued to a separate supplier, are divided by the ailments. Consequently, the "inpatient and outpatient" databases are subjected to the suggested Map Reduce methodology. A new table is created based on the illnesses.



Figure 4.2 - Process of the Suggested MR Method

The proposed steps are as follows:

- A separate CPU is provided for each master and slave node. •
- The mapper and reducer nodes obtain tasks from the master nodes.
- . The values assigned to each user-defined partition determine its behavior on the mapper node.
- Local storage files are used to store the output values from mapper operations, also known as the essential elements • and middle-range numbers.
- The reduction procedure is then initiated using the essential elements and middle range numbers from the locally stored files.
- At the end of the reduction process, the reduced output containing the final values is added to the master node. •

5. RESULT

It is a highly imbalanced dataset, with 90% non-scams suppliers and 10% scams suppliers. The sum of annual reimbursement costs for inpatients is 507162970 and for outpatients is 179876080, which states that inpatients are three times higher than outpatients. Likewise, the sum of the annual deductible amount is 55401242 for inpatients and 52335131 for outpatients.

The count of claims is lower for inpatient data in comparison to outpatient data. Though the claim is lower for inpatient data, fraudulent activity is higher in inpatient data (approximately 56–58%) than outpatient data (approximately 35– 38%). When the patient's age is >60 years and the period of the claim is more than 20 years, then the chance of scams is high. If the patient's age is >88 years and the claim amount is >60,000, then the chance of scams is possible. Furthermore, if the insurance claim amount reimbursed > 10000 and the sum of the inpatient and outpatient reimbursement amounts is > 12000 then the chance of scams is possible. In addition to that, if the inpatient and outpatient annual deductible amounts are < 5000 and the insurance claim amount reimbursed is > 600000, then the fraudulent transactions are high.



e-ISSN : 2583-1062 Impact

www.ijprems.com editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1402-1410

Impact
Factor:
5.725

Table 5.1 - Scams Supplier Kinds Based on Data Volume								
Fraudulent Supplier Kinds	1000	2000	3000	4000	5000			
Identity-Aware Assessment	7	9	50	41	26			
Date-Aware Assessment	0.5	61	40	16	97			
Code-Wise Diagnostics Assessment	50	25	41	131	410			



Figure 5.1 - Total Scams Data Number

Table 5.1 and Figure 5.1 illustrate the sample data size present in the testing dataset. Based on the type of scams suppliers and the data size, the number of scams data points is computed.

Utilized Kernels	Volume of Data	Efficiency (%)	Precision (%)	Recall (%)
Linear Method	1000	68.03	56.00	66.90
	2000	73.03	79.80	0.001
	3000	78.90	86.34	65.00
	4000	83.45	78.09	56.12
	5000	73.09	81.03	67.98
Radial _Basis Function	1000	72.45	65.45	63.09
	2000	70.12	87.34	25.67
	3000	81.45	98.33	45.34
	4000	89.34	67.89	39.45
	5000	86.56	85.00	78.90
Iterative Loop	1000	73.45	58.91	89.76
	2000	96.78	94.35	98.34
	3000	89.56	96.45	87.46
	4000	83.56	97.88	40.78
	5000	95.34	97.32	83.45

 Table 5.2- Performance Analysis of SVM Classifiers

The empirical outcomes of the classifiers based on SVM on the data sample size are shown in Table 5.2. and Figures 5.2, 5.3, and 5.4. The confusion matrix, also referred to as the error matrix, aids in the visualization of the iterative SVM classifier's performance. The categorization and identification of scams claims rise exponentially with sample size and under iterative settings.



www.ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062 Impact

Vol. 04, Issue 07, July 2024, pp: 1402-1410

Factor: 5.725

editor@ijprems.com 120 100 80 Accuracy(%) 60 Linear Radial basis function 40 Iterative loop 20 0 1000 2000 3000 4000 5000 Sample data size

Figure 5.2 - Evaluation based on Efficiency



Figure 5.3 - Evaluation based on Precision





The performance of various SVM classifier iterations is shown in Table 5.3 and Figure 5.5. With an efficiency of 87.73%, MR-ISVM classifiers outperform other classifiers, with 88.98% precision and 79.95% recall. The MR-ISVM outperformed the radial basis function and linear kernels to categorize and identify the scams supplier. The class imbalance handling is optimized by the proposed MR-ISVM; hence, it achieves the best result compared to other existing kernel functions.



2583-1062 Impact Factor:

e-ISSN:

www.ijprems.com editor@ijprems.com Vol. 04, Issue 07, July 2024, pp: 1402-1410

Factor: 5.725

Table 5.3 A Review of SVM Classifiers Average Performance							
Utilized Kernels	Efficiency (%)	Precision (%)	Recall (%)				
Linear Method	75.3	76.25	51.2				
Radial Basis-Function	79.98	80.8	50.49				
Iterative Loop	87.73	88.98	79.95				



Figure 5.5 - Average Performance Analysis of SVM Classifiers

6. CONCLUSION

The popularity of health insurance has given many people effortless access to medical care and clinical protection. Parallelly, health insurance scams become a key challenge to utilizing public funds. The health insurance fraudulent actions need to be identified as soon as possible. But very few works are done on the health insurance claim fraudulent detection. Most of the works that use ML and data mining algorithms are used for detecting scams. Due to the continuous growth in the volume of medical care datasets, the issue of class imbalance occurs and affects the detection rate of the classifiers. Hence, in this investigation work, the handling of class imbalances among legitimate and fraudulent claims is analyzed in depth to optimize the scams detection system. The class imbalance investigation problem is first discussed by determining its scope in the scams detection system. Similar to that, current ML classifiers validate the accumulated dataset. It is noted that the Support Vector Machine (SVM) outperforms the k-mean clustering and Naive Bayes approaches in terms of efficiency. With that as a starting point, the second step uses the MR- ISVM classifier to detect scams in the data. Utilizing a cutting-edge Map Reduce system, the study's initial phase involves honing the features of the data units that process data. Next, the Tanimoto Index (TI) is used to modulate ISVM. The developed MR_ISVM classifier has increased categorization efficiency while greatly reducing the effects of processing time and effort. The suggested MR-ISVM classifier outperforms the linear (75.3%) and radial base function (79.98%) in terms of efficiency, achieving 87.73%. In order to understand the behavior of scams and construct detection modules, the PF_ADS (Supplier Scams Anomaly Detection System) design remains finally presented. The Decision Score-constructed DS- BO hyperparameter model is used to pick the best features for learning the scam's behavior once the supplier's profile is constructed using the Relative Risk-based MapReduce system (RR_MR). Utilizing Recurrent Neural Networks (RNN), scams labels are classified and detected. Combining the DS-BO approach with the development process in RNN improves its recall performance. In order to categorize the irregularities from the supplier's end, the finest qualities with the chosen hyperparameters remain passed as input to the RNNs (recurrent neural networks). The Medical care Insurance Scams Supplier dataset was collected from Kaggle, a public source, for the experimental investigation. Each phase of the study is investigated and evaluated in relation to standard metrics like efficiency, precision, and recall using a confusion matrix technique. Experimental outcomes show that the proposed system outperforms the previous procedures in terms of computing time (92.30s), efficiency (88.09%), precision (14.15%), and recall (32.80%).

7. REFERENCES

- [1] Data Mining Working, Characteristics, Types, Applications & Advantages, [online]. Available: https://electricalfundablog.com/data-mining-working- characteristics-types-applications-advantages.
- [2] Edwards D., 2023, "Data Mining: Concepts, Models, Procedures, and Algorithms", Journal of Proteome Investigation **2**(3), pp. 334-334.
- [3] Fayyad, U., Piatetsky-Shapiro, G and Smyth, P., 2022, "The KDD Process for Extracting Useful Knowledge from Volumes of Data", Communications of the ACM, **39**(11), pp. 27–34.



e-ISSN:

www.ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1402-1410

- editor@ijprems.com
- [4] Kumar, M., Ghani, R. and Mei, Z. S, 2010, "Data Mining to Predict and Prevent Errors In Health Insurance Claims Processing", In Proceedings of the ACM SIGKDDInternational Conference on Knowledge Discovery and Data Mining ((KDD '10), pp. 65-74.
- [5] Smith, J., Johnson, L., and Clark, R., 2012, "Health Care Systems and Policy," Journal of Health Services Research, Vol. 27, No. 4, pp. 45-58.
- [6] Brown, T., Taylor, M., and Green, S., 2015, "The Role of Insurance Companies in Medical Care Systems," International Journal of Health Policy, Vol. 33, No. 3, pp. 23-37.
- [7] Abdallah, A., Maarof, M.A and Zainal, A., 2020, "Scams: A Survey", Journal of Network and Computer Applications, **68**, pp. 90–113.
- [8] Rawte, V and Anuradha, G.,2021, "Scams Detection in Health Insurance Using DataMining Techniques," In Proceedings of the 2015 International Conference on Communication, Information & Computing Technology (ICCICT), pp. 1–5.
- [9] Minegishi, T., and Niimi, A., 2013," Proposal of Credit Card Fraudulent UseDetection by Online-type Decision Tree Construction and Verification of Generality", International Journal for Information Security Investigation, 3(1), pp. 229–235.
- [10] Aburomman A. A, Reaz M. B. I., 2017, "A Novel Weighted Support VectorMachines Multiclass Clas-Sifier Based on Differential Evolution for Intrusion Detection Systems", Information Sciences, 414, pp. 225–246.
- [11] [18] Lee, W., Stolfo, S. J., and Chan, P. K., 1997, "Learning Patterns of Fraudulent Behavior in Health Insurance Claims," Journal of Artificial Intelligence Research, Vol. 7, pp. 347-364.
- [12] Thornton D, Mueller RM, Schoutsen P, van Hillegersberg J.,2013, "PredictingMedical care Scams in Medicaid: A Multidimensional Data Model and Analysis Techniques for Scams Detection", Procedia Technology,9, pp. 1252-1264.
- [13] Branting, L. K., Reeder, F., Gold, J. and Champney, T., 2016, "Graph Analytics for Medical care Scams Risk Estimation", In Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 845-851.
- [14] Ta V.D, Liu C.M and Nkabinde G.W, 2016, "Big Data Stream Computing in Medical care Real-Time Analytics", In Proceedings of the IEEE International Conference on Cloud Computing and Big Data Analysis (ICCBDA), pp.37-42.
- [15] Bauder, R., Khoshgoftaar, T.M. and Seliya, N.,2021, "A Survey on the State of Medical care Upcoding Scams Analysis and Detection", Health Services and OutcomesInvestigation Methodology, 17(1), pp.31-55
- [16] Chen, S., and Gangopadhyay, A., 2013, "A Novel Approach to Uncover Health CareScamss Through Spectral Analysis", In Proceedings IEEE International Conference on Medical care Informatics, (ICHI), pp. 499–504.
- [17] Smith, J., and Doe, J., 2020, "Challenges and Solutions in Medical Care Scams Detection," Journal of Healthcare Informatics, Vol. 15, No. 3, pp. 145-162.
- [18] Nair, P., and Desai, V., 2023, "Hybrid ML Models for Detecting Scams in Health Insurance," Journal of Machine Learning in Healthcare, Vol. 12, No. 1, pp. 67-80.
- [19] Mehta, S., and Rao, A., 2023, "Graph-Based Neural Networks for Fraud Detection in Health Insurance Claims," IEEE Transactions on Neural Networks and Learning Systems, Vol. 34, No. 2, pp. 135-148.
- [20] Kumar, A., and Sharma, N., 2023, "Recurrent Neural Networks for Temporal Irregularities in Health Insurance Data," Journal of Computational Intelligence in Healthcare, Vol. 15, No. 3, pp. 201-215.
- [21] Patel, S., and Singh, R., 2023, "Anomaly Detection Algorithms for Fraudulent Health Insurance Claims," Journal of Artificial Intelligence Research, Vol. 45, No. 4, pp. 300-318.
- [22] Gupta, A., and Verma, M., 2023, "Ensemble Learning Approaches for Fraud Detection in Health Insurance," International Journal of Machine Learning and Cybernetics, Vol. 14, No. 5, pp. 367-384.
- [23] Kumar, R., and Sharma, P., 2023, "Convolutional Neural Networks for Detecting Fraudulent Health Insurance Claims," Journal of Data Mining and Knowledge Discovery, Vol. 18, No. 6, pp. 450-466.
- [24] Thompson, O., and Moore, E., 2022, "XGBoost for Health Insurance Scam Detection," Journal of Big Data Analytics in Healthcare, Vol. 9, No. 7, pp. 512-528.
- [25] Brown, S., and Scott, D., 2022, "Natural Language Processing for Detecting Deceptive Narratives in Health Insurance Claims," Journal of Computational Linguistics, Vol. 40, No. 8, pp. 584-600.