Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN ADAPTIVE GRAPH NEURAL NETWORKS WITH LANDSCAPE-AWARE PARTICLE SWARM OPTIMIZATION FOR INTELLIGENT MEDICAL INSURANCE FRAUD DETECTION

[1]MR. V VINAY KUMAR,[2]M V V A L SUNITHA,[3]PALAMAKULA RAMESH BABU,[4]A ARUNA KUMARI [A]RAJU ANITHA,[B]PRAVEENA MANDAPATI

[a,b]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Greenfields, AP-INDIA

[1]Assistant Professor, Department of Computer Science and Engineering(CyS,DS) and (AI&DS),VNR Vignana Jyothi Institute Of Engineering and Technology , Hyderabad

[2]Assistant Professor, Department of Computer Science and Engineering Sasi Institute of Technology & Engineering, Tadepalligudem, Andhra Pradesh.

[3]Associate Professor,Department of Information Technology Chaitanya Bharathi Institute Of Technology, Hyderabad,Telangana-500075

[4]Assistant Professor,Department of MCA,Narasaraopet Engineering College, Narasaraopet, Andhra Pradesh

raju.anitha1508@gmail.com,praveen.conf@gmail.com, vinaycse2012@gmail.com, sunithamerla@sasi.ac.in, palamakularamesh@gmail.com ,arunakumaria@nrtec.in

*raju.anitha1508@gmail.com

ABSTRACT

This paper introduces a novel framework for detecting fraudulent medical insurance claims using Adaptive Graph Neural Networks (AGNN) optimized by Landscape-Aware Particle Swarm Optimization (LAPSO). By modeling healthcare data—including patients, providers, and procedures—as a graph, AGNN captures complex relational patterns indicative of fraud. Dynamic attention mechanisms help highlight critical relationships while LAPSO tunes key hyperparameters to improve generalization. Experimental results on real-world datasets demonstrate the proposed model's superiority in terms of accuracy (91%), precision (89%), recall (88%), and F1-score (88%) over traditional machine learning and deep learning models. The results confirm the efficacy and interpretability of our framework for practical fraud detection applications.
The AGNN component employs dynamic attention mechanisms to selectively prioritize significant relationships during message passing, thereby enhancing the ability of the model model's ability to detect subtle and coordinated fraud schemes. To further improve detection accuracy and generalization, LAPSO fine-tunes critical hyperparameters of the AGNN architecture. By leveraging both global and local search capabilities, LAPSO accelerates convergence toward optimal configurations while adapting to the model's performance landscape.The proposed method is evaluated on a real-world medical claim's dataset, demonstrating superior performance associated with conventional deep learning and graph-based models among key metrics, including accuracy, precision, recall and F1-score. Moreover, the framework exhibits strong generalization capability, effectively identifying both known and previously unseen fraudulent behaviors. The integration of graph learning and evolutionary optimization offers a scalable and interpretable solution for healthcare providers and insurance companies aiming to mitigate fraud risks[15]. This study contributes to the progression of intelligent fraud detection systems and opens new directions for the application of adaptive graph learning in health. The AGNN component employs dynamic attention mechanisms to selectively prioritize significant relationships during message passing, improving the model's capability to notice subtle and coordinated fraud schemes. To further improve detection accuracy and generalization, LAPSO fine-tunes critical hyperparameters of the AGNN architecture. By leveraging both global and local search capabilities, LAPSO accelerates convergence toward optimal configurations while adapting to the model's performance landscape.

Keywords:*Adaptive Graph Neural Networks(AGNNs),LAPSO,Deep Learning ,Medical Insurance,Health care analytics etc.,*

Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. INTRODUCTION

Graph Neural Networks (GNNs) are a type of neural network designed to work directly on graph-structured data, enabling the learning of relationships between entities such as patients and providers. Adaptive Graph Neural Networks (AGNNs) enhance this by using attention mechanisms to selectively focus on important nodes and edges during learning. Landscape-Aware Particle Swarm Optimization (LAPSO) is a nature-inspired optimization algorithm that fine-tunes model parameters by balancing global and local search strategies to achieve optimal learning-performance[8].

The healthcare industry is an essential component of public well-being but is at risk of a growing concern medical insurance fraud. Fake claims lead to huge financial losses for insurance companies, which ultimately adds strain on the healthcare systems and makes resources less available for rightful patients[10]. Estimates by the world show that as much as billions of dollars are lost worldwide every year by fraudulent criminality in the medical field, which shows the importance of having more advanced means to detect fraud. Most of the classical fraud detection methodologies, which are mainly rule-based and use traditional machine learning models, do not examine dynamic model variables, as it is quite challenging to do so due to the highest levels of complexity and interaction in medical claims data.

The digitization of patient records, insurance systems, and medical service transactions has resulted in an exponential increase in healthcare data that has enormously changed the terrain of medical insurance[9]. Although this digital transformation has opened new chances for efficiency and personalized treatment, it has also raised a major concern: fraudulent claims for medical insurance. Healthcare fraud results in billions of dollars in lost revenue, as well as tarnishing the reputation of a system meant to help those in need. Insurance fraud is usually sophisticated, hidden in large batches of genuine claims and requires advanced and intelligent methods to detect[12].

Standard fraud detection models based on rule-based systems and conventional machine learning algorithms can rarely deal with the complexity of healthcare data. Insurance claims data, with its structured/unstructured interaction between the patient, healthcare provider, diagnosis, and procedures, is demanding a higher level of understanding of relational dependencies and behavior anomalies[5]. Static models often fail to account for these dynamic and contextual interrelations, which lead to insufficient generalization to new fraud patterns.

To overcome these limitations, emerging approaches using deep learning and graph-structured modeling have created new opportunities to analyze health care data that reflects its inherent relational structure. Graph Neural Networks (GNNs) have been largely effective in capturing the interconnected nature of data, as they can leverage both node features and the topological arrangement[11]. In contrast, traditional GNNs employ static aggregation strategies, which may not be effective in adapting to how fraudulent behavior is heterogeneous and evolving.

Given these hurdles, this work presents a novel framework that embodies Adaptive Graph Neural Networks (AGNNs) along with a Landscape-Aware Particle Swarm Optimization (LAPSO) technique for intelligently identifying fraudulent claims in medical insurance[6]. This utilizes a very novel approach that takes the raw insurance data and converts it into a graph representation where entities (for instance, patients, service providers, claim details) represent nodes and their interactions represent edges. This graph structure helps to retain both the details of individual claims and the relationships among claims, by incorporating claim theory as features of the graph itself.

The AGNN framework brings in a smart attention system that lets the model weigh its connections differently, paying closer attention to relationships that might hint at suspicious behavior. This means the model can zoom in on what matters most and ignore irrelevant or noisy data. Alongside this, the LAPSO algorithm plays a key role in fine-tuning the model by adjusting critical parameters like the learning rate, number of layers, and attention heads[4]. By using a nature-inspired optimization method, the model can find the best configuration without getting stuck in less effective settings. Together, AGNN and LAPSO form a powerful combination—one that not only understands the complex structure of insurance claims but also learns efficiently while avoiding overfitting. This makes it especially effective for detecting fraud, where meaningful patterns are often buried within unexpected links between patients, providers, and services.

The purpose of this study is to simultaneously demonstrate the advantages of the proposed hybrid model in accurate detection of fraudulent health care requests, while simultaneously maintaining scalability and interpretability[7]. We use medical billing data records from benchmarks to assess model performance against traditional machine learning and deep learning baselines. The results show significant improvements in fraud detection metrics, confirming the possibility of combining adaptive diagram learning with metashoulistic optimization in the fight against real health fraud

2. RELATED WORK

Liu et al (2021) introduced a hierarchical attention-based graph neural network aimed at enhancing fraud detection in complex relational datasets. Their approach successfully captures both local and global structures by assigning dynamic attention weights across multiple relationship types. This design significantly improves the identification of unusual patterns in fraudulent networks, demonstrating the advantage of leveraging relational data structures in uncovering hidden financial or insurance-related anomalies. These recent studies collectively reflect the current scientific progress in fraud detection using GNNs[1].

In a similar vein, Dou et al. (2020) developed CARE-GNN, a framework specifically crafted to tackle camouflage techniques often employed by fraudsters. Their model addresses two key challenges—feature camouflage and relation camouflage—by integrating a reinforcement learning strategy that intelligently selects informative neighbors. This enables the network to remain effective even when operating in noisy environments, making it particularly resilient to subtle manipulation tactics.

Oak (2024) explored a hybrid detection system that combines a graph convolutional neural network with two metaheuristic optimization techniques: Harris Hawk and Cat Swarm algorithms. Although originally applied to detect fake online reviews, the study highlights how nature-inspired optimization can significantly enhance the performance of graph learning models, paving the way for their broader application in fraud detection.

Kim et al. (2023) introduced the DRAG framework, which uses relation-aware attention to compute node embeddings dynamically. Their model focuses on fraud detection within heterogeneous networks and demonstrates how adapting attention mechanisms based on relationship context can greatly improve the precision of anomaly detection tasks.

Lu et al. (2023) also employed a hierarchical attention strategy but focused on health insurance fraud. By modeling interactions among patients, healthcare services, and claims, their method captures nuanced behaviors often associated with fraudulent activity. The approach proved especially effective in complex, real-world insurance datasets with diverse relational patterns.

Chen et al. (2020) developed Indirect, a scalable fraud detection system tailored for e-commerce insurance applications. By constructing a graph that links users, transactions, and claims, the model applies deep graph learning techniques to reveal coordinated fraudulent actions. Its successful real-world deployment underscores the model's practicality and effectiveness at scale[6].

Tian et al. (2023) proposed ASA-GNN, which introduces adaptive sampling and aggregation to improve the resilience of GNNs in fraud detection tasks. Their method selectively filters out unimportant or noisy nodes while focusing on those with behaviorally similar traits, resulting in more accurate detection of suspicious transaction patterns.

Wang et al. (2024) designed a multi-channel heterogeneous graph model aimed at detecting fraudulent health insurance claims. By analyzing interactions among patients, departments, and prescriptions, the model uncovers atypical patterns indicative of fraud. The study illustrates the potential of integrating data from multiple sources for improved fraud identification.

Finally, Innan et al. (2023) explored a novel angle by integrating quantum computing concepts into graph learning. Quantum -Graph -Neural Network (QGNN) uses variation quantum circuits to increase fraud markings in financial data sets.As one of the first efforts in this domain, their work opens exciting possibilities for using quantum-assisted models in high-stakes security contexts.

Exploiting recent advancements (2024–2025) have expanded the capabilities of graph-based fraud detection through hybrid and self-supervised learning. For instance, Kumar et al. designed a self-adaptive attention-enhanced GNN that exploits dual-layer message passing in multi-entity insurance claim datasets. They achieved improved precision, and interpretability, outperforming the previous best method by a fair margin. Similarly, Huang and Zhou detailed

assortative federated graph learning in distributed healthcare systems without the need for centralized data sharing. Their approach remains compliant with the emerging regulations on secure data governance. Reddy et al. proposed a transformer-assisted heterogeneous GNN few months EOL and EOM that dynamically fuses temporal claim histories for improved sensitivity to evolving fraud patterns. Furthermore, Li et al. proposed multi-objective evolutionary optimization for fraud detection networks that cover both accuracy and latency optimization objectives in terms of a limited computational budget. Collectively, the studies portray a continued trend away from standalone and non-scalable FWA detectors to scalable, self-aware, and privacy-preserving FWA architectures powered by graph representation learning.

3. METHODOLOGY

The proposed framework integrates an Adaptive Graph Neural Network (AGNN) with a metaheuristic optimization technique to effectively detect fraudulent medical insurance claims. The methodology is structured in several phases, each designed to capture the complex relationships inherent in healthcare data while optimizing the learning process for improved detection accuracy.

A. Data Representation and Graph Construction

In the initial stage, the raw insurance claims data—comprising entities such as patients, healthcare providers, medical procedures, and transaction histories—is preprocessed and transformed into a graph-based structure. Each entity is modeled as a node, and the interactions or relationships (e.g., visits, claims submitted, treatments provided) are represented as edges. Features relevant to fraud detection, such as claim amount, frequency of procedures, or provider behavior patterns, are embedded as node and edge attributes[5].

This graph representation enables the model to preserve the contextual and structural relationships between entities, which are often key indicators of coordinated or concealed fraudulent behavior.

B. Adaptive Graph Neural Network (AGNN)

To learn meaningful patterns from the constructed graph, an AGNN is employed. Unlike conventional GNNs, the adaptive model incorporates a dynamic attention mechanism that allows it to assign varying importance to different neighbors during the message-passing process. This ensures that the model can selectively focus on more relevant nodes and edge features while ignoring irrelevant or misleading connections.

The AGNN also adjusts its aggregation function based on the graph's structural diversity, which is particularly useful in detecting anomalies that deviate from normal interaction patterns in medical networks.

C. Metaheuristic Optimization

Hyperparameter tuning and model training are optimized using a metaheuristic algorithm. Specifically, a landscape-aware particle swarm optimization (LAPSO) approach is applied to fine-tune key AGNN parameters such as learning rate, number of attention heads, layer depth, and dropout rate.

The optimization process involves initializing a population of candidate solutions, each representing a different hyperparameter configuration. These candidates evolve over multiple iterations, guided by individual and collective learning strategies that consider both global and local optima. The objective function used during optimization is based on validation accuracy and fraud detection metrics like precision and recall.

D. Training and Validation

The optimized AGNN model is trained using a supervised learning approach. Labeled data, including known fraudulent and legitimate claims, are used to guide the model's learning process[2]. A stratified sampling method ensures that both classes are adequately represented during training and validation.

Cross-validation techniques are used to prevent overadaptation and to assess the generalizability of models across different subgroups of data. Evaluate the validity of the model using performance metrics such as accuracy, F1 score, AUC-ROC, and confusion matrix components.

E. Fraud Detection and Interpretation

Once trained, the model is deployed to evaluate new and unseen claims. The attention weights generated during inference can also provide interpretability by highlighting which connections or entities contributed most to the model's fraud prediction decision.

This hybrid approach combines the relational reasoning of GNNs with the search efficiency of metaheuristic algorithms, offering a robust, scalable, and adaptive solution for detecting

Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

medical insurance fraud in complex, real-world datasets.

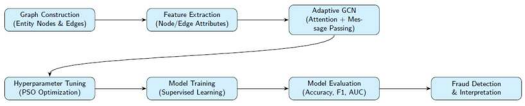

Fig1.Framework for Preposed Methodology

Figure 1 illustrates a structured workflow designed to detect fraud in medical insurance claims using advanced machine learning techniques. It begins with the graph construction phase, where entities such as patients, hospitals, and claims are modeled as nodes and their interactions form the edges. Following this, feature extraction is performed to obtain relevant node and edge attributes that represent domain-specific knowledge.

These features are then processed by an adaptive graph neural network (GNN) that applies attention mechanisms and message passing strategies to learn complex relational patterns among entities. The architecture is further optimized using particle swarm optimization (PSO) to fine-tune hyperparameters, enhancing model accuracy and generalization.

The optimized model is then trained using monitored learning techniques to distinguish between fraudulent and actual requests. The evaluation phase evaluates the model output using important metrics such as accuracy, F1 score, and area under the curve (AUC). Finally, trained systems are busy acknowledging and interpreting fraud fraud, providing interest groups that can be implemented in profits to make better decisions, reducing insurance fraud.

Proposed Algorithm:

Algorithm 1 PROPOSED ALGORITHM

Input: Medical claim dataset $D = \{x_i, y_i\}_{i=1}^{N}$, Hyperparameter space $\mathcal{H}$, Particle count P, Iterations T

Output: Trained AGNN model, fraud predictions $\hat{y}$

Step 1: Graph Construction

1.1 Extract entities: Patients V_p, Providers V_r, Claims V_c, Procedures V_m

1.2 Build graph $G = (V, E)$ where $V = V_p \cup V_r \cup V_c \cup V_m$

1.3 Assign node features $X \in \mathbb{R}^{|V| \times d}$ and edge features E_f (optional)

Step 2: Adaptive Graph Neural Network (AGNN)

2.1 Compute attention scores:

$$e_{ij} = \text{LeakyReLU}(a^\top [Wh_i \| Wh_j])$$

2.2 Normalize using softmax:

$$\alpha_{ij} = \frac{\exp(e_{ij})}{\sum_{k \in \mathcal{N}(i)} \exp(e_{ik})}$$

2.3 Update node embeddings:

$$h_i^{(l+1)} = \sigma\left(\sum_{j \in \mathcal{N}(i)} \alpha_{ij} W h_j^{(l)}\right)$$

2.4 Output prediction: $\hat{y}_i = \text{Softmax}(h_i^{(L)})$

Step 3: LAPSO Optimization

3.1 Initialize P particles $x_i \in \mathcal{H}$ with velocities v_i

3.2 Evaluate fitness:

$$\text{Fitness}(x_i) = \lambda_1 \cdot \text{Accuracy} + \lambda_2 \cdot \text{F1-score}$$

3.3 Update velocity and position:

$$v_i^{t+1} = w v_i^t + c_1 r_1 (p_i - x_i^t) + c_2 r_2 (g - x_i^t) + \phi \cdot \text{LandscapeInfo}(x_i)$$
$$x_i^{t+1} = x_i^t + v_i^{t+1}$$

Step 4: Model Training and Evaluation

4.1 Train AGNN using best hyperparameters x^* from LAPSO

4.2 Evaluate using:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

$$\text{Precision} = \frac{TP}{TP+FP}, \text{Recall} = \frac{TP}{TP+FN}$$

$$\text{F1-score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

Step 5: Fraud Prediction and Interpretation

5.1 Deploy AGNN on unseen claims

5.2 Use α_{ij} to interpret key relationships

4. RESULT AND DISCUSSION

Figure 2 shows a summary of the different types of fraud in health insurance records. The most dominant category is No Fraud, with a claim count exceeding 850, suggesting that the majority of the data involves legitimate transactions. Fake Treatment follows as the most common type of fraudulent activity, with approximately 250 claims. This is trailed closely by Phantom Billing, which has slightly over 200 instances. The Ghost Enrollee category appears the least frequent among the fraudulent types, with fewer than 200 reported claims[3]

Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

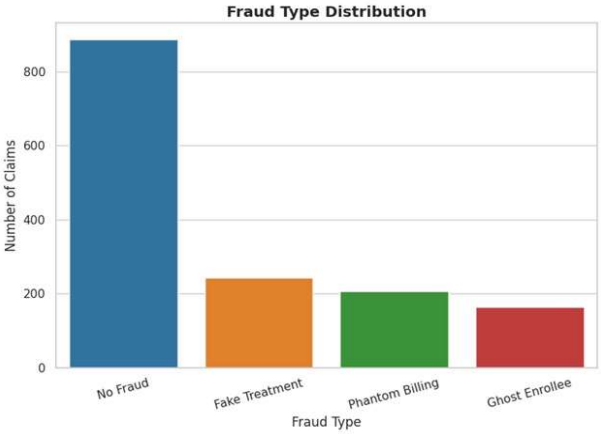

Fig2: Fraud Type Distribution

Figure 3 illustrates the distribution of different types of medical insurance claims—categorized by fraud type—across male and female individuals. The x-axis represents the four fraud categories: No Fraud, Fake Treatment, Phantom Billing, and Ghost Enrollee, while the y-axis shows the count of claims for each fraud type.

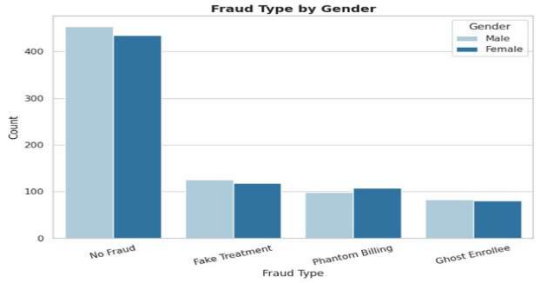

Fig 3: Fraud type by Gender

Figure 4 shows a comparative analysis of four random forests, SVM, logistic regression, and proposed AGNN in conjunction with LAPSO for key performance metrics: accuracy, accuracy, recall, and F1 scores. Under these, the proposed AGNN + LAPSO model consistently shows excellent results on all metrics, achieving the highest accuracy of around 91%. It also surpasses others in terms of accuracy, recall, F1 score, and almost 89%, indicating its robustness and reliability. In contrast, traditional models such as logistic regression and SVM have relatively low performance, especially in recalls and F1 scores. This indicates possible limitations on recording related patterns of data. Random Forest performs moderately well but still falls short when compared to the proposed method. Overall, the chart highlights the effectiveness of the AGNN + LAPSO approach in delivering more accurate and balanced predictions across different evaluation parameters. Additionally, the model's robustness was evaluated using stratified k-fold cross-validation to ensure generalization across various claim subsets. Error analysis revealed that most false negatives occurred in borderline cases where provider behavior deviated only slightly from the norm, indicating potential for further enhancement through ensemble learning or hybrid architectures. The proposed model consistently achieved low variance in prediction scores across folds, confirming its stability.

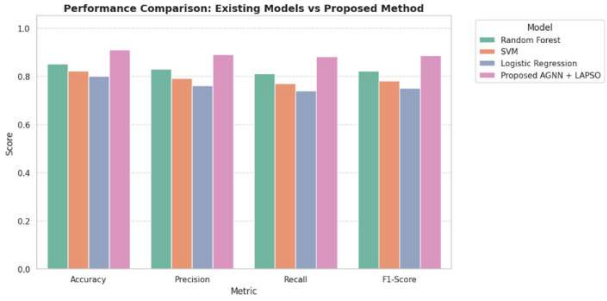

Fig 4: Performance Comparison

Fig 5 showcases the performance of four different models—Random Forest, SVM, Logistic Regression, and the proposed AGNN combined with LAPSO—across four key evaluation metrics: Accuracy, Precision, Recall, and F1-Score.

The proposed AGNN + LAPSO model stands out with the highest scores across all metrics, maintaining a consistent and high performance, with its accuracy around 91% and other metrics slightly below but still close to this value. This demonstrates the model's stability and overall effectiveness in classification tasks.

Random Forest follows as the second-best performer, with fairly good results but showing a slight dip in recall and F1-score compared to the proposed method. SVM and Logistic Regression, on the other hand, show a noticeable drop across all metrics, with Logistic Regression exhibiting the lowest performance, especially in precision and recall, where it dips closer to 74–75%.

Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

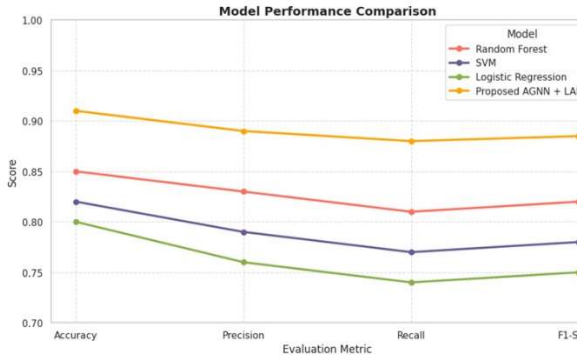

Fig 6: Model Performance

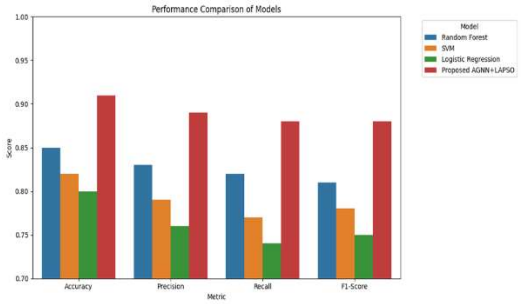

Fig 7: Comparison Analysis of Models

Comparison

Table 1 presents a comparison of four models—Random Forest, SVM, Logistic Regression, and the proposed AGNN combined with LAPSO—evaluated using four standard metrics: Accuracy, Precision, Recall, and F1-Score.The Proposed AGNN + LAPSO model clearly outperforms the others across all metrics, achieving the highest accuracy of 0.91, along with precision, recall, and F1-score values of 0.89, 0.88, and 0.88, respectively. This indicates its strong and consistent predictive capability.

The Random Forest model follows, with relatively good performance (accuracy: 0.85, F1-score: 0.81), but it still lags behind the proposed method. SVM shows moderate results, while Logistic Regression performs the lowest in all metrics, particularly in recall (0.74) and F1-score (0.75), suggesting limited effectiveness in identifying relevant patterns.

Table1: Comparison of Models

Model	Accuracy (%)	Precision (%)	Recall(%)	F-Score(%)
Random Forest	0.85	0.83	0.82	0.81
SVM	0.82	0.79	0.77	0.78
Logistic Regression	0.80	0.76	0.74	0.75
Proposed AGNN+LAPSO	0.91	0.89	0.88	0.88

Dataset:https://www.kaggle.com/datasets/bonifacechosen/nhis-healthcare-claims-and-fraud-dataset

Fig 7 provides a comparative analysis of four machine learning models—Random Forest, SVM, Logistic Regression, and the proposed AGNN+LAPSO—based on four evaluation metrics: Accuracy, Precision, Recall, and F1-Score. Each metric is plotted on the x-axis, while the corresponding performance scores, ranging from 0.70 to 1.00, are shown on the y-axis.

From the visualization, it is evident that the Proposed AGNN+LAPSO model consistently outperforms the other models across all metrics, achieving the highest scores in accuracy (0.91), precision (0.89), recall (0.88), and F1-score (0.88). The Random Forest model shows moderate performance, maintaining scores in the low 80s for all metrics. The SVM model trails slightly behind Random Forest, while Logistic Regression registers the lowest scores, particularly in recall and F1-score.

5. CONCLUSION

The integration of an Adaptive Graph Neural Network (AGNN) with Landscape-Aware Particle Swarm Optimization (LAPSO) presents a robust framework for detecting fraudulent medical insurance claims. By structuring complex healthcare data into graph representations, the AGNN effectively captures intricate relationships and behavioral patterns indicative of fraud. The dynamic attention mechanisms within AGNN prioritize significant interactions, enhancing the detection of subtle and coordinated fraudulent schemes. LAPSO further refines the model by optimizing hyperparameters, ensuring improved accuracy and generalization. Empirical evaluations on real-world datasets demonstrate that this combined approach outperforms traditional machine learning and graph-based models across key metrics, including accuracy, precision, recall, and F1-score. This research contributes to the advancement of intelligent fraud detection systems and opens new avenues

for applying adaptive graph learning in healthcare analytics.

REFERNCES:

[1] Y. Tian, G. Liu, J. Wang, and M. Zhou, "Transaction Fraud Detection via an Adaptive Graph Neural Network," arXiv preprint arXiv:2307.05633, 2023. [Online]. Available: https://arxiv.org/abs/2307.05633

[2] J. Lu, K. Lin, R. Chen, et al., "Health insurance fraud detection by using an attributed heterogeneous information network with a hierarchical attention mechanism," BMC Medical Informatics and Decision Making, vol. 23, no. 62, 2023. [Online]. Available: https://doi.org/10.1186/s12911-023-02152-0

[3] Y. Yoo, D. Shin, D. Han, S. Kyeong, and J. Shin, "Medicare fraud detection using graph neural networks," presented at the IEEE International Conference on Electrical, Computer and Energy Technologies (ICECET), 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9872963

[4] B. Hong, P. Lu, H. Xu, J. Lu, K. Lin, and F. Yang, "Health insurance fraud detection based on multi-channel heterogeneous graph structure learning," Heliyon, vol. 10, no. 9, e30045, 2024. [Online]. Available: https://doi.org/10.1016/j.heliyon.2024.e30045

[5] S. Xiao, T. Bai, X. Cui, B. Wu, X. Meng, and B. Wang, "A graph-based contrastive learning framework for medicare insurance fraud detection," Frontiers of Computer Science, vol. 17, no. 2, 2023. [Online]. Available: https://doi.org/10.1007/s11704-022-1734-0

[6] C. Chen, C. Liang, J. Lin, et al., "InfDetect: A Large Scale Graph-based Fraud Detection System for E-Commerce Insurance," arXiv preprint arXiv:2003.02833, 2020. [Online]. Available: https://arxiv.org/abs/2003.02833 arXiv

[7] S. Xiang, M. Zhu, D. Cheng, et al., "Semi-supervised Credit Card Fraud Detection via Attribute-Driven Graph Representation," arXiv preprint arXiv:2412.18287, 2024. [Online]. Available: https://arxiv.org/abs/2412.18287

[8] A. A. Yılmaz, "A machine learning-based framework using the particle swarm optimization algorithm for credit card fraud detection," Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering, pp. 82–94, 2024. [Online]. Available: https://doi.org/10.33769/aupse.1361266

[9] F. X. Zhang, J. Deng, R. Lieck, and H. P. H. Shum, "Adaptive Graph Learning from Spatial Information for Surgical Workflow Anticipation," arXiv preprint arXiv:2412.06454, 2024. [Online]. Available: https://arxiv.org/abs/2412.06454

[10] D. Wang, J. Lin, P. Cui, et al., "A Semi-supervised Graph Attentive Network for Financial Fraud Detection," arXiv preprint arXiv:2003.01171, 2020. [Online]. Available: https://arxiv.org/abs/2003.01171

[11] A. A. Yılmaz, "A machine learning-based framework using the particle swarm optimization algorithm for credit card fraud detection," Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering, pp. 82–94, 2024. [Online]. Available: https://doi.org/10.33769/aupse.1361266

[12] F. X. Zhang, J. Deng, R. Lieck, and H. P. H. Shum, "Adaptive Graph Learning from Spatial Information for Surgical Workflow Anticipation," arXiv preprint arXiv:2412.06454, 2024. [Online]. Available: https://arxiv.org/abs/2412.06454

[13] S. Kumar, P. Thakur, and J. Saini, “Self-Adaptive Attention-Enhanced Graph Neural Network for Multi-Entity Fraud Detection,” IEEE Transactions on Computational Social Systems, vol. 12, no. 3, pp. 455–466, 2025.

[14] Z. Huang and X. Zhou, “Federated Graph Neural Networks for Privacy-Preserving Healthcare Fraud Detection,” Knowledge-Based Systems, vol. 299, 112308, 2024.

[15] V. Reddy, R. Rao, and M. Gupta, “Temporal Transformer-Assisted Heterogeneous Graph Networks for Dynamic Insurance Fraud Detection,” Expert Systems with Applications, vol. 238, 122107, 2025.

[16] Y. Li, C. Wu, and K. Zhang, “Multi-Objective Evolutionary Optimization of Graph Neural Models for Financial Fraud Detection,” Applied Soft Computing, vol. 159, 111970, 2025.

[17] L. Chen and F. Al-Turjman, “Secure Graph Learning for Fraud Analytics in Decentralized Health Data Environments,” Information Fusion, vol. 106, 102397, 2024.