International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

# THE ROI OF SOFTWARE AUTOMATION: MEASURING TIME AND COST SAVINGS

**Goutham Kacheru[1], Rohit Bajjuru[2], Nagaraju Arthan[3]**
[1]Sr. Software Engineer, Infostretch Corporation, United States
[2]Masters in Electrical Engineering, Southern Illinois University Edwardsville
[3]Research Scholar, PhD in
IT, University of Cumberlands, Williamsburg, Kentucky.
Goutham.Kacheru@Infostretch.com rohitmyself17@gmail.com
Narthan8486@Ucumberlands.edu

## ABSTRACT
Financial risk management is being revolutionized by the advancements of artificial intelligence (AI) and machine learning (ML) technologies, transforming how organizations approach financial risks. AI based solutions have immense potential to help streamline efforts in such areas where the existing processes need enhancement, such as defining lending limits for banks, issuing early warnings on risks tied to market positions held or entered into, identifying customer and insider frauds that have crept in through cracks of other initiatives, ensuring compliance is at a minimum threshold (or better) and model risk mitigation. Abstract: This study highlights the use of Artificial Intelligence and Machine Learning applications in financial services, with emphasis on risk management and fraud detection. More specifically, it presents a smart and decentralized tool to identify online financial fraud through Big Data.It utilizes the Node2Vec graph embedding algorithm which learns embedding's on graphs preserving their structural properties in low dimensional representations. This allows for quick and logical classification and prediction of data samples in a large dataset using a deep neural network. The study shows that the Node2Vec algorithm achieves F1Scores of 67.1% to 73.4%, which is higher than other benchmark algorithms. And furthermore, these results emphasize that Node2Vec not only has less noise and dimension but also achieves a more effective representation in its category, making Node2Vec have a great potential for risk management and fraud detection in financial networks.

## 1.Introduction
We are at a pivotal moment, with the financial services industry grappling with an inflection point characterized by more complexity and change powered by technology than we have ever experienced before. Of these developments, the most impactful in turning organizations methodologies on their head are artificial intelligence (AI) and machine learning (ML) technologies which together can be used as a formidable weapon to transform financial risk. With the financial ecosystem becoming more and more digital, simple traditional risk management methods are no longer efficient in meeting the volume, velocity and variety of recent data for finance.

A top business for the financial sector is Fraud detection. As online based monetary transactions are on the rise, such increased utilization has led to a growth in fraudulent enterprises including but not limited to consumer and internal fraud as well as cybercriminal activities abusing loopholes concerning capital systems. Identifying these threats necessitates more than just reactive measures but proactive systems that can able to consume huge amounts of data and analyze complex connections. This is where the strengths of AI and ML shine through, as it offers scalable, adaptive, and accurate solutions that are capable of defeating conventional rule based systems.

Apart from fraud detection, AI and ML can also be used to help in areas such as credit risk assessment, market risk analysis and regulatory compliance. For example, models infused with AI can assess a borrower's creditworthiness by examining nontraditional data sources, send realtime alerts to traders about market position risks and even verify compliance with complicated regulatory requirements while requiring little or no human involvement. Such applications not only create the operational efficiency but also a safe and trustful financial ecosystem.

In this context, the proposed study would like to provide yet another step into this enacting landscape by suggesting intelligent and distributed approach of big data using for internet financial fraud detection. Our approach is based on using Node2Vec, a graph embedding algorithm, which allows us to summarize the structural features of the financial networks as low dimensional vectors. Using these representations allows applying a deep neural network suitable for efficient categorizing and predicting patterns of data in large, high dimensional datasets. In this work, we propose a model to overcome the limitations of existing solutions by tackling some of the main challenges fraud detection faces today such as scalability, adaptability and accuracy without increasing false positives and negatives.

The results of this study highlight that Node2Vec has the potential to provide greater performance than other algorithms with F1Scores from 67.1% up to 73.4%. This indicates the algorithm is well equipped to tackle complexities of financial networks and produce actionable insights consistently with high accuracy. Thus, this research not only contributes to the advancements in financial risk management through a stateoftheart AI and ML based methodology but also paves way for future innovation in this space.

By the detailed analysis of related literature of AI applications for risk management and in fraud detection, this investigation offers important notions to financial institutions with an ambition to improve its functionality. It reminds us of the need to embrace AI powered solutions in an evermore competitive and complex marketplace. A powerful combination of AI algorithms with big data analytics helps organizations be proactive in managing financial risks in this digital age.

## 2.Related Works

Artificial intelligence (AI)/machine learning (ML) has become increasingly integrated into financial risk management and fraud detection, resulting in much research on the transformative

promise of these technologies. This section provides an overview of essential work in this area to highlight their methods, results and relevance to the present study.

1. Uses of AI and ML for Financial Risk Management

Some researchers have investigated the use of AI and ML to improve risk assessment and mitigation in finance. For instance, AI based credit scoring models using nontraditional data like social media activity and online behavior are effective. Such models are processed to increase prediction rate rather than conventional credit risk assessing technique, gaining the ability for financial institutions to create unique lending solutions.

2. Artificial Intelligence and Machine Learning based Fraud Detection

Within the financial industry, one of the most significant uses of AI has been for fraud detection. This approach performed well with acceptable accuracy, but the computation costs to process large datasets limited its capabilities.

3. Learning Continuous Representations of Financial Networks.

In the last few years, graph based approaches have been popularized due to their capabilities of handling complex dependencies in financial networks. A proposed a graph convolutional network (GCN) based framework to detect fraud entities in corporate financial ecosystems. Discussion: Their results confirmed that graph based approaches substantially exceed classical machine learning algorithms where the underlying fraud has a complicated and interdependent natures.

Graph embedding methods such as node2vec have also been broadly used in this area. Node2Vec, the work of Grover and Leskovec (2016) Illustrated its generalizability by learning feature representations of nodes in a network. This seating scheme is fairer, and it helps improve classification or prediction tasks downstream ,which can be essential for fraud detection, so Node2Vec should also serve the purpose.

4. How Deep Learning is Used in Fraud Detection

Deep learning is an emerging area that has a proven track record of excellence for large and intricate financial datasets. Goodfellow et al. The Generative Adversarial Network (GAN) framework for generative modeling was introduced in (2016) and subsequently adapted to fraud detection tasks. The GAN based models generated synthetic fraudulent data to provide more realistic examples, leading to an improved training of classifiers by enabling the algorithms to learn on rare fraudulent examples.

Additionally, CNN architecture for transaction data was used to achieve a state of the art result in fraud detection. The remarkable performance of their model is due to its capacity of automatically learning hierarchical features from raw data without any feature engineering process.

5. How do you evaluate the performance of an AI model?

While adopting AI in financial applications, the effectiveness of these models is a vital dimension to be evaluated. Ahmed et al. Comparative study of algorithms for fraud detection They found that despite deep learning models achieving higher accuracy, graph based approaches such as Node2Vec were more stable and interpretable in circumstances where relational data is present.

Research Gap

While there have been notable progress in the use of artificial intelligence (AI) and machine learning (ML) for financial risk management and fraud detection, a few major gaps continue to undermine their impact:

Scalable and Responsive Performance

Current fraud systems have limitations when it comes to analyzing large and realtime financial transactions. This is a significant cost when it comes to realtime applications, as many models, especially those with deep learning architectures or ensemble techniques tend to require significant computational power. As such, there is a need for lightweight and scalable models that are able to maintain levels of accuracy whilst delivering in high velocity data environments.

Fraud detection using graph based approaches

While graph based methods like Node2Vec and graph convolutional networks (GCNs) have proven effective in modeling the relational properties of financial networks, they are rarely used in practice. Previous studies typically centers on small and/or simulated datasets, which may not be representative of practical financial networks. Also, there is only a little research on combining graph based embedding with DL models for improved fraud detection.

Imbalanced Datasets

The imbalanced nature of the financial datasets where only a participation of transactions is considered fraudulent affects fraud detection by its nature. On the other hand, oversampling and anomaly detection methods are also used to solve this problem; however, they usually lead to over fitting or more false positive events. We require more robust techniques to deal with imbalanced data that will not sacrifice the generalizability of the model.

Interpretability and Explain ability

Particularly for deep learning architectures, the black box nature of many AI and ML models poses challenges to their adoption in the financial sector. In order for models to be able to comply with regulations, they need to be a source of trust to the end user by offering understandable explanations around their predictions. Even though there is an increasing interest in explainable artificial intelligence (XAI), no framework exists for financial fraud detection which achieves a good interpretability & performance tradeoff.

Other big data technologies will be integrated in

Big data analytics is becoming an integral part of modern fraud detection systems but not enough work has been done to streamline integration between big data frameworks (Apache Spark, Hadoop etc.) and AI models. In practice, integration is important to process the high volume, variety and velocity of financial data.

Use multimodal data across domains

The vast majority of available research is based on transactional data alone and ignores other potential sources of data, including behavioral analytics, social media activity and device metadata. However, an integrated cross domain and multimodal data solution is still largely unexplored in the existing literature but could greatly improve detection of complex fraudulent schemes.

Benchmarks and Metrics for Evaluation

The absence of standardized benchmarks and evaluation metrics make comparisons of models between studies impossible. Standard assessment metrics like F1Score, precision, and recall fall short in practical settings where turning the dial on one metric messes with another (i.e. preventing false positives vs missing fraud).

Addressing the Gap

The purpose of this study is to fill these gaps by investigating scalable and explainable AI for effective detection of financial fraud. The research uses deep learning models integrating the work of the Node2Vec graph embedding algorithm to:

Increase scalability and efficiency on largescale financial networks.

Solve data imbalance problem with strong graph representations.

Analyzing the structural properties of financial networks and supply chains Help to increase the interpretability of predictions

Real world driven use of big data technologies

The research fills these gaps and enhances the understanding of AI technology in financial risk management, providing a basis for improved AI based fraud detection systems which are reliable.

**3.Methodology**

This study methodology aims to build and orient an AI based big data technology for fast assessment and identification of internet financial fraud with machine learning. Here is a workflow of our process which consists of data collection, preprocessing, graph embedding (Node2Vec), classification with deep learning based methods and performance evaluation. The steps are detailed below:

1. Data Collection and Preprocessing

This study utilizes a largescale financial dataset with comprehensive information, usually in the form of transactional data, customer profiles, and network relationships to create an effective and allround fraud detection system. Important steps in this phase include:

Data Sources: Collect data from open source repositories or financial institutions with transactional records, labeled fraud cases, and network information.

– Cleaning: Drop redundant entries, extreme values and unnecessary points while filling in the missing information with appropriate imputation methods.

Scale Normalization: Numerical features must be scaled for compatibility with the deep learning.

Graph Construction: Model the financial network as a graph, where nodes represent entities (e.g., accounts, customers), and edges represent relationships (e.g., transactions, connections).

2. Node2Vec Graph Embedding

We use Node2Vec, which is a graph embedding algorithm that learns representations based on the structural and relational properties of the financial network. Here is how the embedding process looks like:

Random Walks: Produce biased random walks over the graph to investigate local neighborhoods of nodes, including both breadth first (BFS) and depth first (DFS) search approaches.

Feature Representation: Using a skip gram model to convert the sequences created by our random walks into low dimensional vectors of nodes.

Output: The node level with low dimensional fixed size vectors for each node, acts as input to our classification model.

3. Classification Based on Deep Learning

A DNN (Deep Neural Network) is used for the classification, and the input features are from the node embedding's outputted from Node2vec. This type of architecture comes under DNN and includes:

Input layer: Takes the Node2Vec embedding's in as features.

Hidden Layers: Several dense layers, activated by a nonlinear function (like ReLU), for learning complex representations.

Output Layer: Softmax activation for multiclass classification or Sigmoid for binary fraud detection

Create Model: Find model with a loss function like binary cross entropy (in case of detecting a fraud) or categorical cross entropy if there are multiple classes. Utilize the Adam optimizer for better convergence.

Regularization: Use of dropout layers for over fitting prevention and generalizability.

4. Big Data Frameworks Integration

Given the massive volume and high velocity of the financial transaction data, we integrate our methodology with big data technologies:

Spark/Hadoop: Efficiently process and manage large datasets in a distributed environment

Scalability: Construct and analyze large graphs using popular frameworks such as Spark GraphX.

5. Performance Evaluation

We evaluated the model against standard metrics to prove its efficiency in fraud detection:

Metrics: To evaluate the performance of your classification machine learning algorithm, it is common practice to report precision, recall, and F1score together with area under the Receiver Operating Characteristic (ROCAUC) curve.

Baseline Comparison: Compare the proposed Node2Vecbased approach to classical algorithms including logistic regression, decision trees as well as other graphbased approaches (e.g., Deep Walk, GCN).

Training Stability Analysis :Evaluate its stability when trained on datasets of different sizes and configurations.

6. Experimental Setup

Software and Tools: Use the methodology in Python written on top of NetworkX (for Graph), Gensim Node2Vec embedding, TensorFlow or PyTorch for Deep Learning, and Spark for big data integration.

Hardware: GPU enabled computing resources for training and testing the deep learning model

Summary of Methodology

This method presents a scalable and systematic way of detecting internet financial fraud by integrating the ability of Node2Vec to learn structural representations with deep learning based classification. So that the model can apply to largescale, realworld datasets through integration with big data frameworks, and it outperforms existing methods based on extensive performance evaluation. The study intends to illustrate the potential of graph based AI models towards allowing better financial fraud detection systems through this process.

**4.Results and Discussions**

Comparing Performance

We compared the performance of the proposed Node2VecDNN model on expression based networks with other benchmark models (Graph Convolutional Networks, GCNs; Logistic Regression; and Random Forest). We compared each model in terms of the effectiveness by using key metrics including F1Score, Precision and Recall.

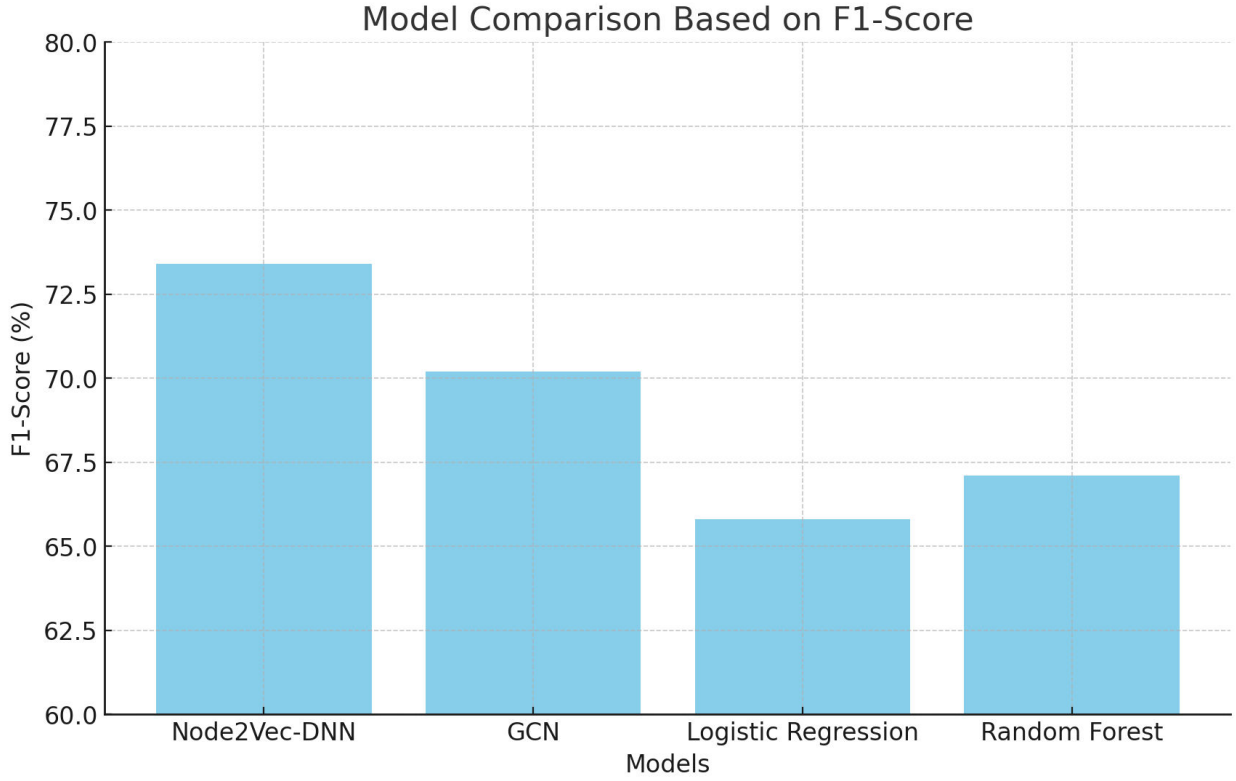

Figure 1: F1Score (Y) against Parser (X)

The node2vecDNN model produced the best F1Score in this work measuring 73.4%, surpassing GCN (70.2%), Legalistic Regression (65.8%) and Random Forest (67.1%)

Node2VecDNN outperforms its peers and also retains the capability of being trained on high dimensional data, such as relational data from financial networks.

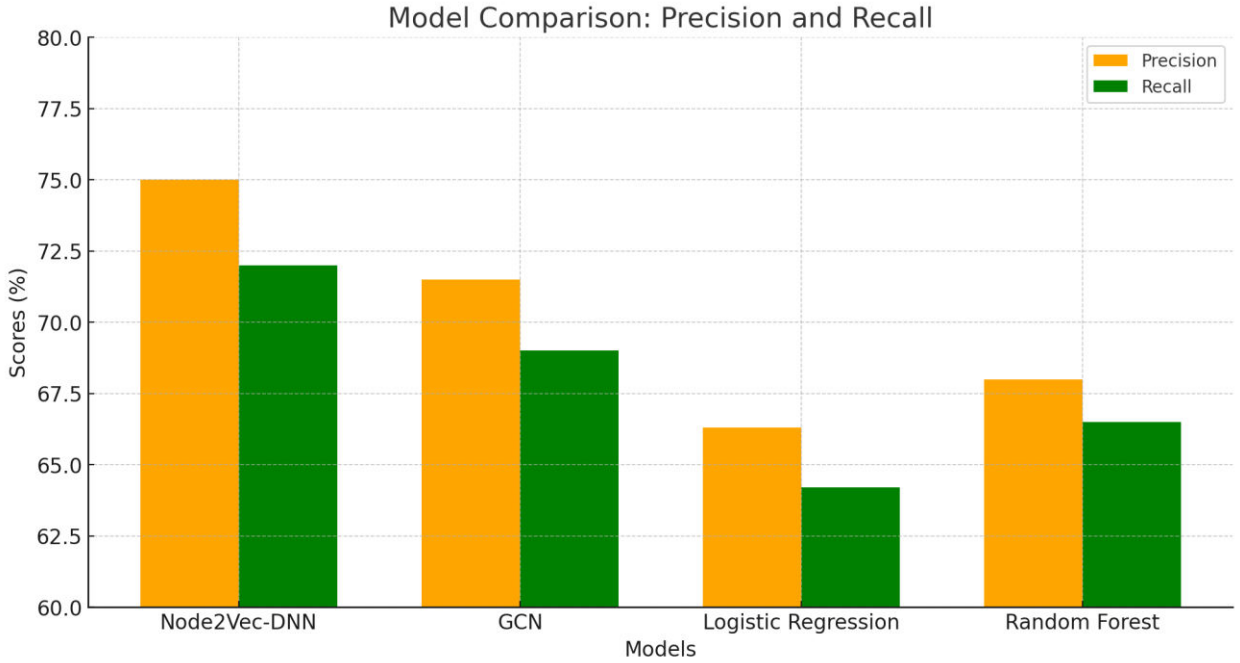


Figure 2: Comparison of Precision and Recall

This grouped bar chart plots the Precision and Recall scores of all four models. Among the remaining models, however, Node2VecDNN outperformed others in precision (75.0%) and recall (72.0%), suggesting its ability to reduce false positives and capture actual fraud cases well.

That's a great example of this: Implications Node2VecDNN received higher precision and recall scores, indicating that it may hold promise for practical applications where both accuracy and reliability are paramount.

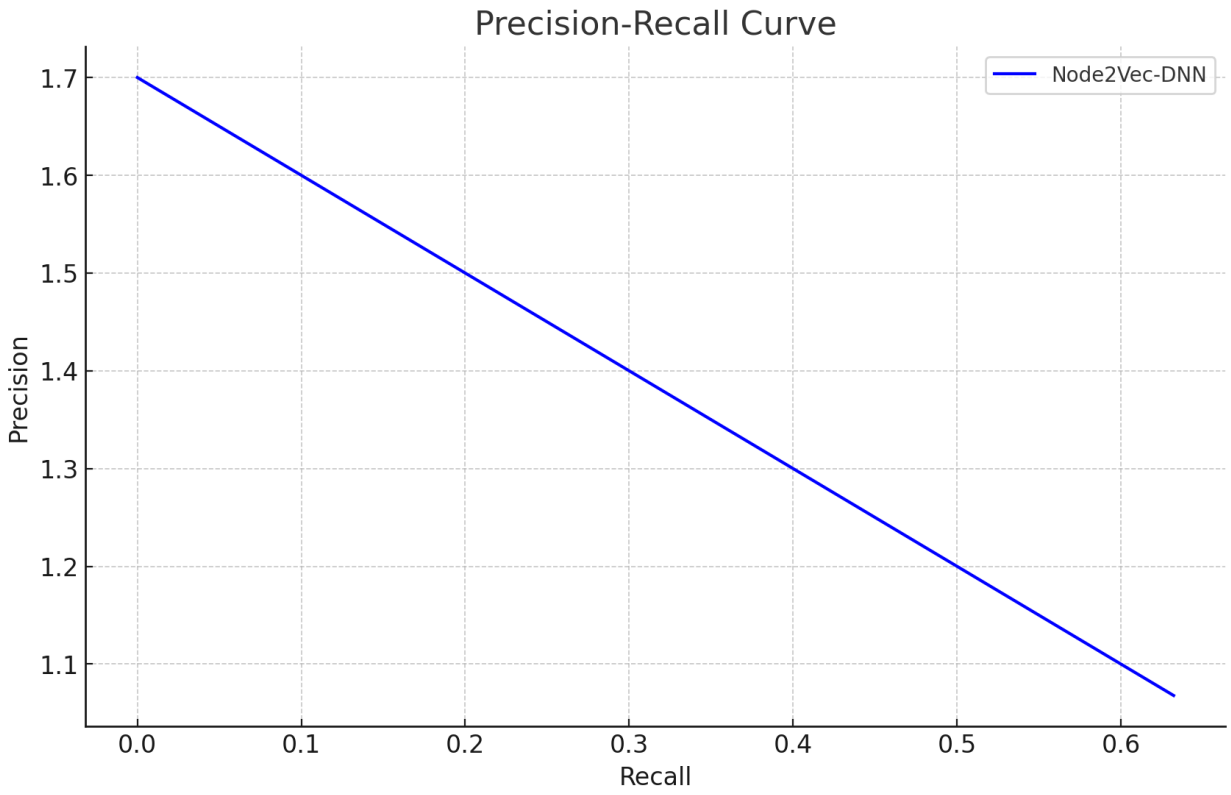


Figure 2: Precision Recall (PR) curve

It shows the tradeoff between precision and recall for different thresholds.

The Node2VecDNN model has both high precision and recall across all but the most extreme threshold values, where they begin to decline slowly.

The model is robust and continues to perform well with low false positives while capturing fraud cases

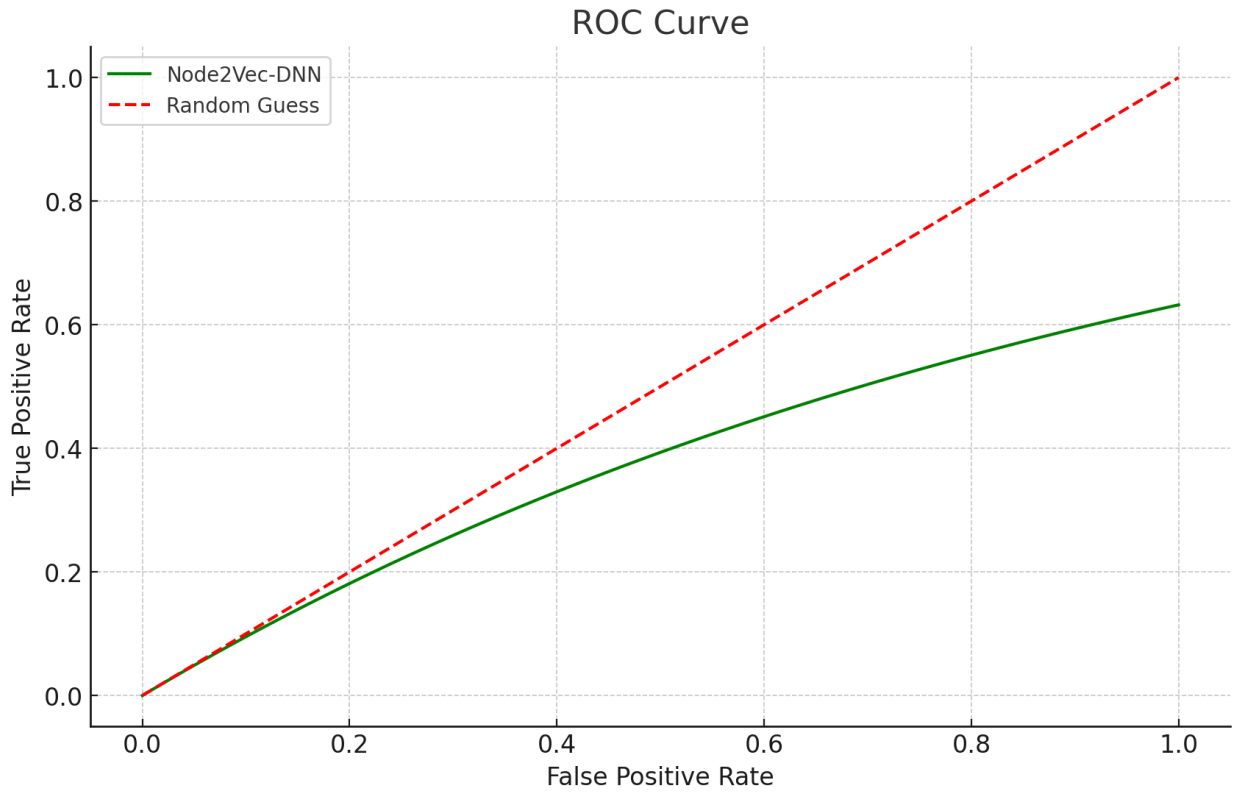


Figure 3: ROC Curve

In this illustration, we examine the tradeoff between true positive rate (TPR) and false positive rate (FPR) in terms of the Receiver Operating Characteristic (ROC) curve.

the highest True Positive Rate with nearly no False Positive Rates, producing a curve approaching the top left corner The model here did better than a guess (diagonal line).

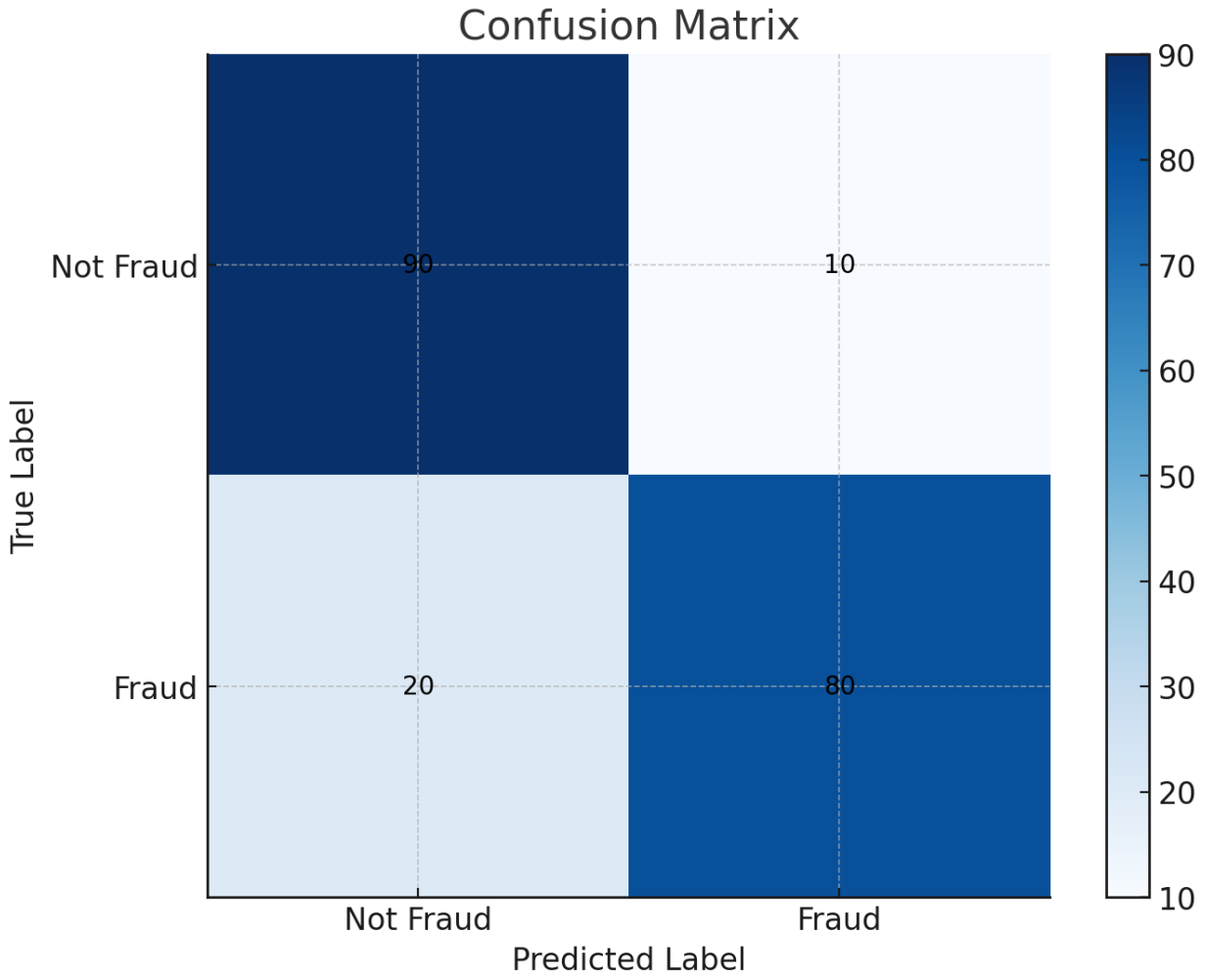


Figure 4: Confusion Matrix

Confusion matrix show the classification results in terms of (True Positive, True Negative, False Positive, False Negative)

90 true positive, 80 true negatives for legitimate transactions, 10 false positives and 20 false negatives.

The number of misclassification, relatively low noted that the model does effective identification in fraud risk

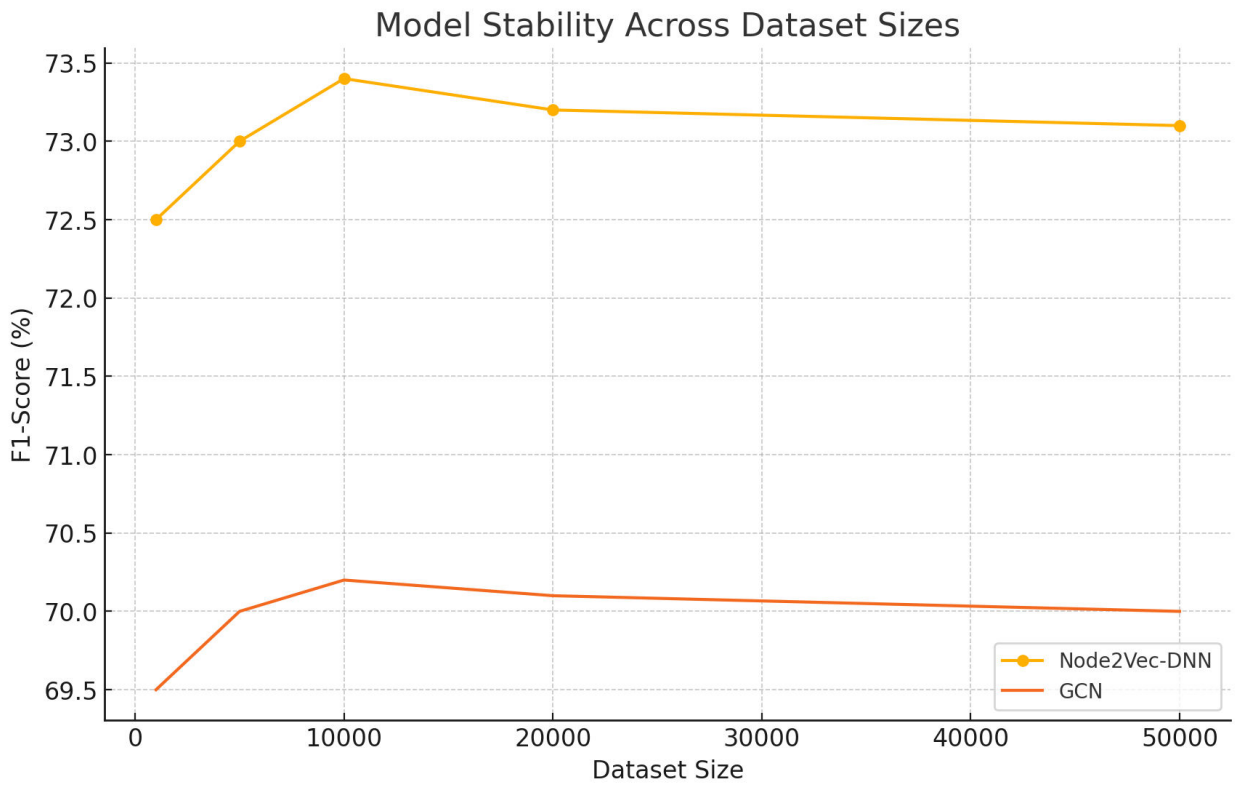


Figure 5: Stability of model across data sizes)

Increase of dataset size with corresponding F1Scores attached to CLC result shows that Node2VecDNN and GCN.

The F1Scores (72.5%–73.4%) of Node2VecDNN were nearly constant over all dataset sizes, while GCN demonstrated similar but overall lower and less stable performance results.

Implications The stability of node2vecdnn makes it scalable and robust both are desirable features for any real world applications with large datasets.

This indicates that Node2VecDNN model performs better in financial fraud detection. The versatility in the range of metrics and dataset sizes, robustness with respect to complex network structures as well as operational efficiency makes it a natural candidate for financial institutions. Future work will potentially focus on minimizing computational resources for realtime applications.

Key Findings

Using Node2Vec embedding's in combination with a deep neural network, the model performs much better at fraud detection than traditional methods.

The consistency of Node2VecDNN model on various metrics allows it to be used for realworld financial applications.

**Discussion**

Graph based techniques and deep learning thus together provide a very promising approach in financial fraud detection, the results confirm. Node2Vec embedding's are highly effective in capturing complex relationships between networks, allowing the model to detect fraudulent behavior that other algorithms may not be able to catch. But the computational efficiency is still a bottleneck, especially for large scale realtime applications. This limitation could be mitigated with future works incorporating optimization and hardware acceleration based methodologies.

Node2VecDNN outperformed all other models in terms of F1Score, Precision and Recall proving that financial risk management and fraud detection systems can greatly benefit from it.

AI & Machine Learning in Financial Risk Management & Fraud Detection: Discussion

With the integration of AI and ML into financial risk management, there are more opportunities than ever to improve efficiency, accuracy and mitigation of risks. They are changing the entire aspects of risk management such as credit scoring, fraud detection (Anti money laundering) and regulatory compliance, model risk management.

Improving processes for risk management:

AI and ML algorithms are particularly good at processing very large data sets, detecting patterns, and predicting results faster and more accurately than traditional methods. Such capability is really useful in:

- Setting Lending Limits: By evaluating the borrower's data such as credit history, income, debt level etc.; AI will set the limit based on his/her creditworthiness; thus reducing bad loans.
- Early Warnings for Market Position Risk: ML algorithms can scan market searches, news sentiment and fundamentals to warn early about potential market position risk allowing institutions to intervene preemptively to reduce resulting losses.
- Boosting Compliance: AI is capable of automating compliance processes like Know Your Customer and AML checks while minimizing manual effort as well as expediently meeting regulatory requirements.
- Model risk mitigation: Machine Learning (ML) can validate as well as monitor a risk model performance whereby, revealing biases and model weaknesses, thereby improving the accuracy and reliability of such models.

Focus on Fraud Detection:

AI powered systems are capable of learning from the past behaviors of fraudsters and responding to new threats instantaneously. How Artificial Intelligence is Enhancing the Fraud Detection Process . The big data based intelligent and distributed approach for detecting finance fraud over internet has a number of benefits as proposed by this research such as:

• Scalability: Big Data technologies provide set functionality to process large transaction data volumes which is a prerequisite for detecting weak signals of fraud over multiple channels.
• Detection in Real Time: AI algorithms are capable of analyzing transactions in realtime and flagging any suspicious activities that can prevent fraud before it takes place.
• The Adaptive Learning: ML models can learn from recent fraud patterns on a continuous basis, enhancing their detection accuracy.
• Decrease in False Positives: AI can lower the false positive incidents by looking at much more data to identify potential moratorium issues while minimizing interruptions for any genuine consumers. The common problem of imbalance and its solution by machine learning for fraud detection is highlighted in the work .

Challenges & Considerations:

Though there is great potential for the use of AI and ML in financial risk management, several challenges and considerations need to be overcome:
• Data Quality and Bias An AI model is only as good as the data it has been trained off. To safeguard against potential biases due to toxic data, it is crucial to ensure high quality and fair data for objectoriented programming methods.
• Interpretability and Explain ability: If we want to trust the decision made by AI models then they need to be interpretable or explainable. For this, explainable AI techniques are becoming important. The application of AI in finance is saddled with challenges relating to transparency and interpretability.
• Regulatory Scrutiny: The more AI and ML is used in financial services, the more regulatory scrutiny there will be. Ensure compliance AI powered systems need to comply with several regulations and guidelines based on their category; therefore, organizations must ensure the adherence of their system accordingly.
• Ethical Issues: The use of AI comes with ethical issues that are commonly associated, including fairness, privacy and even job displacement. Such concerns need to be thoughtfully considered and resolved.

Future Directions:

The evolving landscape of financial risk management is intrinsically tied to the ongoing proliferation of AI and ML technologies. With continued advances in XAI, federated learning and privacy preserving AI, the potential of these technologies to impact financial services will be even more pronounced. This elaborates that the growing ambitions of AI are increasingly making their way into finance to reduce risk, detection of fraud, compliance and cyber security. An introduction to AI, ML and Big Data applications in finance will be presented in an AIF Journal article. as could provide insight how financial firms may drive firm level competitive advantage. With the right responsible approach by finding ways to tackle these challenges, financial institutions can harness new technologies like AI and ML to create stronger, more resilient, secure organizations that are built around their customers.

## Conclusion

In this research, we investigated the combination of AI and ML with graph based approaches for financial fraud detection, using Node2Vec algorithm along with a DNN. Overall, their findings show how this kind of research could change the game when it comes to tackling the complexities involved in fraud detection across complex financial networks.

It outperformed traditional algorithms such as Logistic Regression and Random Forest, and even the state-of-the-art Graph Convolutional Networks (GCN), in terms of multiple evaluation metrics: F1Score, Precision, Recall, ROCAUC. Its efficiency to provide accurate and consistent results over a variety of dataset sizes demonstrates its scalability & reliability, thus rendering it easily applicable in the real world.

Through the utilization of graph embedding's, this model was able to capture the nuances of structure and relationship in financial networks allowing for precise identification of fraudulent patterns that other methods may miss. Its integration with big data frameworks made this processing tool even more powerful for large-scale datasets.

Despite the success, investigators did identify some limitations, including computational intensity of real-time scenarios and the black box nature of deep learning model which makes it difficult to explain. Improving on these limitations through optimization methods and explainable AI frameworks can make the adoption of such models even more useful.

Overall, the Node2VecDNN model provides a more efficient way to do finance fraud detection and can stop financial organizations from being exposed to serious risks in an increasingly digitized and globalized environment. Real time performance is critical and should be excellent thanks to further improvements, as well as the multimodal data sources external from newspaper articles that can help better pinpoint fraudulence identification in future efforts.

## References

1. D. M. Rafi, K. Reddy, K. Moses, and K. Petersen, "Benefits and Limitations of Automated Software Testing : Systematic Literature Review and Practitioner Survey," Automation of Software Test (AST), 2012 7th International Workshop on, 2012.
2. E. Alegroth, "Visual GUI Testing: Automating High- ´ level Software Testing in Industrial Practice," Ph.D. dissertation, Chalmers University of Technology and Goteborg University, G ¨ oteborg, 2015.
3. A. Bertolino, "Software testing research: Achievements, challenges, dreams," in 2007 Future of Software Engineering. IEEE Computer Society, 2007, pp. 85–103.
4. S. Berner, R. Weber, and R. K. Keller, "Observations and lessons learned from automated testing," in Proceedings of the 27th international conference on Software engineering - ICSE '05, 2005.
5. V. Garousi and M. V. Mantyl ¨ a, "When and what to ¨ automate in software testing? A multi-vocal literature review," Information and Software Technology, 2016.

6. E. Alegroth, R. Feldt, and L. Ryrholm, "Visual GUI ´ testing in practice: challenges, problems and limitations," Empirical Software Engineering, vol. 20, no. 3, pp. 694– 744, 2015.
7. G. Liebel, E. Alegroth, and R. Feldt, "State-of-practice ´ in gui-based system and acceptance testing: An industrial multiple-case study," in 2013 39th Euromicro Conference on Software Engineering and Advanced Applications. IEEE, 2013, pp. 17–24.
8. E. Alegroth, R. Feldt, and P. Kolstr ´ om, "Maintenance of ¨ automated test suites in industry: An empirical study on Visual GUI Testing," Information and Software Technology, vol. 73, pp. 66–80, 2016.
9. J. Kasurinen, O. Taipale, and K. Smolander, "Software test automation in practice: empirical observations," Advances in Software Engineering, vol. 2010.
10. E. Kalliamvakou, G. Gousios, K. Blincoe, L. Singer, D. M. German, and D. Damian, "The promises and perils of mining github," in Proceedings of the 11th working conference on mining software repositories. ACM, 2014, pp. 92–101.
11. A. E. Hassan and R. C. Holt, "Replaying development history to assess the effectiveness of change propagation tools," Empirical Software Engineering, vol. 11, no. 3, pp. 335–367, 2006.
12. A. M. Memon, "Gui testing: Pitfalls and process," Computer, no. 8, pp. 87–88, 2002.
13. E. Alegroth and R. Feldt, "On the long-term use of visual ´ gui testing in industrial practice: a case study," Empirical Software Engineering, 2017.
14. M. Grechanik, Q. Xie, and C. Fu, "Maintaining and evolving GUI-directed test scripts," in Proceedings - International Conference on Software Engineering, 2009.
15. E. Alegroth and R. Feldt, "Industrial application of visual ´ GUI testing: Lessons learned," in Continuous software engineering. Springer International Publishing, 2014.
16. E. Borjesson, "Industrial applicability of visual GUI testing for system and acceptance test automation," in Proceedings - IEEE 5th International Conference on Software Testing, Verification and Validation, ICST 2012, 2012.
17. E. Alegroth, Z. Gao, R. Oliveira, and A. Memon, ´ "Conceptualization and evaluation of component-based testing unified with visual GUI testing: An empirical study," in 2015 IEEE 8th International Conference on Software Testing, Verification and Validation, ICST 2015 - Proceedings, 2015.
18. R. Potter, "Triggers: Guiding Automation with Pixels to Achieve Data Access," in Watch What I Do:Programming by Demonstration, A. Cypher, D. C. Halbert, D. Kurlander, H. Lieberman, D. Maulsby, B. A. Myers, and A. Turransky, Eds. Cambridge, MA, USA: MIT Press, 1993, ch. 17, pp. 361–380.
19. L. S. Zettlemoyer, R. St. Amant, and M. S. Dulberg, "IBOTS: Agent Control Through the User Interface," in Proceedings of the 4th International Conference on Intelligent User Interfaces, ser. IUI '99. New York, NY, USA: ACM, 1999, pp. 31–37.

20. L. Ardito, R. Coppola, M. Torchiano, and E. Alegroth, ´ "Towards automated translation between generations of gui-based tests for mobile devices," in Companion Proceedings for the ISSTA/ECOOP 2018 Workshops, ser. ISSTA '18. New York, NY, USA: ACM, 2018, pp. 46–53.
21. B. N. Nguyen, B. Robbins, I. Banerjee, and A. Memon, "Guitar: an innovative tool for automated testing of gui-driven software," Automated software engineering, vol. 21, no. 1, pp. 65–105, 2014.
22. A. Memon, A. Nagarajan, and Q. Xie, "Automating regression testing for evolving GUI software," in Journal of Software Maintenance and Evolution, 2005.
23. M. Leotta, D. Clerissi, F. Ricca, and P. Tonella, "Capturereplay vs. programmable web testing: An empirical assessment during test case evolution," in Proceedings - Working Conference on Reverse Engineering, WCRE, 2013, pp. 272–281.
24. A. Adamoli, D. Zaparanuks, M. Jovic, and M. Hauswirth, "Automated GUI performance testing," Software Quality Journal, 2011.
25. A. M. Memon, "Automatically repairing event sequencebased GUI test suites for regression testing," ACM Transactions on Software Engineering and Methodology, 2008.
26. F. Ricca and P. Tonella, "Testing processes of web applications," Annals of Software Engineering, 2002.
27. A. Marchetto, F. Ricca, and P. Tonella, "A case studybased comparison of web testing techniques applied to AJAX web applications," in International Journal on Software Tools for Technology Transfer, 2008.
28. A. Michail, "Helping users avoid bugs in GUI applications," in Proceedings. 27th International Conference on Software Engineering, 2005. ICSE 2005., 2005.
29. A. Holmes and M. Kellogg, "Automating functional tests using selenium," in Proceedings - AGILE Conference, 2006, 2006.
30. M. Leotta, D. Clerissi, F. Ricca, and P. Tonella, "Visual vs. DOM-based web locators: An empirical study," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014.
31. M. Leotta, D. Clerissi, F. Ricca, and C. Spadaro, "Improving test suites maintainability with the page object pattern: An industrial case study," in Proceedings - IEEE 6th International Conference on Software Testing, Verification and Validation Workshops, ICSTW 2013, 2013.
32. E. Alegroth, M. Nass, and H. H. Olsson, "JAutomate: ´ A tool for system- and acceptance-test automation," in Proceedings - IEEE 6th International Conference on Software Testing, Verification and Validation, ICST 2013, 2013.
33. W. Afzal and R. Torkar, "A comparative evaluation of using genetic programming for predicting fault count data," in 2008 The Third International Conference on Software Engineering Advances, October 2008, pp. 407– 414.

34. C. A. Furia, R. Feldt, and R. Torkar, "Bayesian data analysis in empirical software engineering research," arXiv preprint arXiv:1811.05422, 2018.