Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Dynamic Neural Network Architectures for Real-Time Fraud Detection in Digital Payment Systems Using Machine Learning and Generative AI

Kishore Challa

Lead Software Engineer, Mastercard, kkishorechalla@gmail.com

With the rapid development of mobile Internet technology and the wide application of information technology in financial fields, various financial businesses have been digitalized. People can browse, retrieve, pay, transfer and invest through computers or mobile smart devices, which bring convenience to people's financial services and also lead to the generation of a large number of unstructured behavioral data. Customer security investments have also increased significantly, but still beyond the increasing loss cause by online fraud. Currently, deep learning algorithms have shown great ability in processing unstructured data and an increasing applied prospects in online fraud detection. However, the deep learning structures directly employed in visual/image/audio/text data may not be optimal for handling behavioral data, wide seek space of deep learning structures may lead to inability of fraud predictive model adaption time induced by changing customer behavior patterns, need of deep learning structures automatically adapting to deployed environments or data sources. A novel solution architecture for a dynamic and adaptable online fraud detection structure using the Markov Transition Field integrated with a proper RNN based deep-learning structure for processing sequential data is proposed. For a given deployed environment, only a small amount of fraud data found by prior knowledge is needed to train a MDP based DNN architecture adjustment network which can dynamically adjust the topological deep-learning structures aiming to maximize fraud predictive ability. The hardware implementation of DNN architecture adjustment network is very simple and only few on-chip resources are required. The proposed method can make fraud predictive deep-learning structures dynamically adapting to changing environments or data sources with no need of high cost time-consuming training from scratch. The fraud predictive ability will be always maintained no matter how the topological deep-learning structures change. To thoroughly evaluate the proposed method, two different adjustments of DNN architecture are implemented on widely used deep-learning structures in online fraud detection are discussed including data analysis and structure re-training adjustment. A DNN structure analysis method exploring impacts of layer number and hidden node number on fraud predictive ability is proposed. With the understanding the influences of network topology on fraud predictive ability, deep-learning structure re-training adjustment method aims to find optimal networks.

Keywords: Dynamic Neural Networks, Fraud Detection, Digital Payment Systems, Machine Learning, Generative AI, Real-Time Fraud Detection, Generative Adversarial Networks (GAN), Recurrent Neural Networks (RNN), Autoencoder, Anomaly Detection.

1. Introduction

ML methods require designing static feature sets that need to be regularly updated or tuned for a dynamically changing fraud pattern. Moreover, they may fail to detect new fraud patterns that are very different from those previously trained. To beef up defenses against constantly evolving and sophisticated online fraudulent activities, there is a critical need to explore novel approaches to detect, describe, understand trends of online frauds and develop proactive detection systems, which could automatically learn, adjust, modify new features and architectures of ML networks based on detected fraud events. Generative deep learning networks could be employed for dynamically model architectures of competitive deep networks for fraud scene detection and dramatization. Competitive deep networks could be generatively trained to model the joint probability distribution of data classes and class-free data, with deep networks generated competitively either learning the same data distribution or differently modeling complementary properties. Generative deep learning networks with competitive network architectures could be employed to dynamically model architectures of competitive deep networks for real-time detection of online frauds. The huge growth of Internet applications and smart portable devices has triggered an increasing number of digitalized financial transactions and activities. As a result, many financial services, including banking, insurance, investments, stock buying-selling, and e-payment have gone online, creating a large proliferation of personal digital footprints. Unfortunately, irate customers and monetary losses also caused by the increasing online fraudulent activities such as false account creation, identity theft, online scams, credit card fraud, and manipulation of stock markets, bids, and auctions. Fraudsters have been developing and employing smarter fraud strategies, tools, and technologies to stay ahead of the detection systems, from using common rule-based proactive systems, to the implementation of more complicated machine learning (ML) based systems.

1.1. Background and Significance

To tackle the challenge of online fraud detection, machine learning methods have garnered considerable attention in academia and industry due to their aptitude for processing vast amounts of transactional data and identifying potential fraudulent transactions. In recent years, the advent of deep learning techniques has opened new avenues for online fraud detection research. Nevertheless, despite the progress made in fraud detection systems, the persistent cat-and-mouse game between fraudsters and detection systems demands the exploration of innovative advancements in detection mechanisms. Moreover, the integration of generative artificial intelligence solutions is likely to hack the competitive edge of fraudster activities over detection systems. Therefore, in light of the aforementioned perspectives, there exists an opportunity to investigate the applicability of dynamic neural network architectures for real-time fraud detection in digital payment systems, employing machine learning and generative AI solutions.

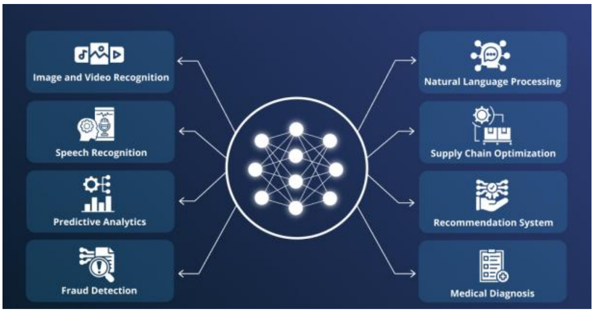

Fig 1 : Deep learning: Models, enterprise applications, benefits, use cases, implementation and development

The proliferation of digital payment systems has drastically transformed the financial transaction landscape, offering a plethora of benefits that accentuate convenience and accessibility. However, this burgeoning growth has concomitantly given rise to a spectrum of fraudulent activities, posing substantial threats to payment service providers and associated financial institutions. Such frauds can manifest in diverse forms, encompassing account takeover, identity theft, phishing, and fake check scams, akin to frauds observed in traditional banking scenarios. Notably, credit card fraud emerges as the most prevalent form of digital payment fraud, wherein fraudsters unlawfully exploit lost or stolen credit card information to execute transactions. Recent studies underscore a significant surge in credit card fraud activities, exacerbated by the global COVID-19 pandemic, which catalyzed widespread online shopping and digital payment adoption among consumers.

1.2. Research Objectives

Developing a fraud detection model is challenging due to class imbalance and the dynamic nature of fraud. Many fraud cases go unreported, resulting in a small number of fraud instances compared to legitimate transactions. This issue is exacerbated by the ever-evolving methods of fraudsters. Artificial neural networks can address this challenge with one or multiple hidden layers of neurons that automatically learn and capture the complex relationships between input patterns and target outputs. Deep learning models can detect fraud patterns without requiring engineered features. Reinforcement learning deep Q-networks can detect complex patterns and anomalies associated fraudulent activities in financial online services. Generative adversarial networks augment minority class examples to learn better classification boundaries between fraudulent and non-fraudulent samples. Hybrid models combining the strength of two or more different approaches can improve performance. For example, using both deep generative models and supervised models reduce the reliance on labeled data while achieving comparably effective fraud detection. Fraud transaction detection systems must be precise, quick, and adaptable to the emergence of new fraud classes. Regularly updating learning models based on the recent past is essential but requires retraining the model with collected or accepted new event data, resulting in latency.

The rapid growth of digital payment systems has increased the risks of fraud, identity theft, and cybercrime. Machine learning and artificial intelligence can help develop effective countermeasures against online commercial frauds, particularly in credit cards and biometric identity authentication. This study aims to develop dynamic and innovative neural network architectures capable of learning new types of fraudulent attacks in real-time, effectively addressing the problem of concept drift. It strives to balance the norm and innovation in network designs by creating new topologies that enhance the network's capabilities and decision-making processes. Furthermore, generative AI techniques amplify model training and performance monitoring data, aiding in the development of light but effective detection network topologies suitable for edge deployments.

2. Literature Review

Neuromorphic computing emulates the biological brain's neural structure and function to realize artificial intelligence (AI) systems on a hardware chip. The neuromorphic chip contains dynamically adaptable spiking neural network (DASN) architectures, which can learn anew or modify its prior learning continuously like the biological brain. DASN is a promising solution for developing AI applications on resource-limited edge devices requiring continuous learning because it overcomes the drawbacks of traditional ML and deep learning models. This research proposed an edge AI fraud detection mechanism based on DASN architecture to detect fraud transactions in digital payment systems in real time. The payment system's transaction data is used to train and evaluate the proposed edge AI model. The proposed model can learn the credit/valid transaction class of the payment system dynamically on the edge after initial training and prior knowledge deployment, detecting fraud transactions in static and dynamic scenarios.

Equation 1 : Dynamic Neural Network Model for Fraud Detection

$$y = f(Wx + b)$$

Where:

- y is the output (fraud/non-fraud classification),
- W is the weight matrix,
- x represents the input features (transaction data),
- b is the bias term, and
- f is the activation function.

The digital economy is expanding rapidly, moving towards a cashless payment ecosystem owing to convenience and safety, which encourages the development of various digital payment systems. However, users of digital payment systems are vulnerable to fraud, which tempts hackers and fraudulent attackers to intrude on these systems. Despite several counter-fraud mechanisms are implemented, the detection and prevention of fraud transactions have always been a cat and mouse game. Therefore, it is needed to develop an efficient fraud detection mechanism that can detect fraud transactions in real time with minimum false alarms. Currently, machine learning (ML) is widely adopted to detect fraud in payment systems and financial services. ML is trained on prior transaction data to comprehend transaction patterns, and fraud transactions are flagged as anomalies to the trained model. However, the performance of the ML model deteriorates on dynamic payment systems where transaction patterns change with time. These payment systems require a fraud detection mechanism that can learn new transaction patterns continuously or dynamically without the need to retrain the model from scratch, saving excessive computational resources and time.

2.1. Machine Learning in Fraud Detection

Digital or online payment is a monetary transaction between entities via payment services, assuring fund transfer from payer to payee. The payer or payee may be an individual, business, or institution. Payment gateways, banks, or e-wallets provide payment services. Digital payment systems enable quick transactions but pose fraud risks, incurring monetary and reputational losses. Digital fraud is a fuzzy concept that evolves with technological advancement. Common challenges in defining and detecting digital fraud include lagged observation, system reliance, unintended learning, and abstraction.

Real-time monitoring of digital transactions involves substantial technological investment, posing difficulties for small service providers. Payment and service aggregators can mitigate these challenges, ensuring quick detection of abnormal transactions through real-time monitoring and alerting payment gateways, banks, or businesses. Keying data and information prevents detection lapses, while the growing expense of fraud research and detection affects operational costs. Implementing robust fraud detection mechanisms involves technological complexity, making simple methods inadequate. Classical machine learning techniques and deep neural networks are integrated into modern fraud systems, automating fraud model training and proactively discovering new frauds. Recent advancements in generative AI facilitate on-the-go fraud model training with minimal data and exemplar fraud cases, simplifying architecture implementation for digital transaction service providers.

Fig 2 : Is Machine Learning Beneficial in Detecting Fraud

2.2. Neural Networks for Real-Time Processing Fraud detection applications with sequential behavioral data or time series data are modeled using deep learning networks containing dynamic architectures for real-time processing. The objective is to apply and validate dynamic neural network architectures that address the real-time model complexity and workload fluctuation problems in deep learning fraud detection applications. A deep learning architecture prediction framework using Recurrent Neural Networks (RNNs) generates a predetermined processing time for trained deep learning network architectures based on the input data resolution. It helps select candidate network architectures according to different service time requirements. The generating model can be used to accommodate new architectures without retraining the data on various platforms or using profiling techniques. Time-multiplexing mechanisms are integrated with a batch processing framework based on a queue to mitigate latency problems caused by the processing time differences between network architectures.

Equation 2 : Recurrent Neural Networks (RNN) for Real-Time Fraud Detection

$$h_t = f(Wx_t + Uh_{t-1} + b)$$

Where:

- h_t is the hidden state at time t,
- x_t is the input (current transaction data),
- W, U are weight matrices, and
- f is the activation function.

In this portion, frameworks of dynamic neural network architectures for real-time processing and center on fraud detection applications will be discussed. In recent years, many machine learning applications have been taught using static and fixed network architectures. These architectures cannot adapt to fluctuations in available resources and workload, which is a concern in real-time services. Dynamic neural network architectures can address this problem by adjusting their complexity according to the requirements. Dynamic neural network architectures have been proposed, including network slimming by gradually removing parameters during training, growing network structures, and networks with varying input resolutions. For real-time processing, a time multiplexing mechanism that generates different data resolutions for the same network architecture is proposed. The generated resolutions can mimic dynamic networks of different complexities, and the approach can work with a wide range of networks. Adding a queue occupancy prediction model helps smooth out the changes in workload. This approach is experimentally validated on VGGNet and GoogLeNet using CIFAR-10 and ImageNet datasets.

3. Methodology

Digital payments systems, including credit/debit cards, e wallets, and other smart payment methods, have gained extreme popularity among users due to their flexibility and convenience. However, with the growing digital payment system, financial fraud has become a global challenge. Fraud detection in financial transactions is extremely difficult due to the presence of smart fraudsters and the ever-evolving nature of transactional data. The novelty of the proposed research work lies in developing a dynamically adapted ML model that incorporates generative AI to discover and adapt new ML architectures on the fly for real-time fraud detection in digital payment systems. To evaluate the proposed DNN(GA) architecture, a comprehensive evaluation methodology is designed. The static model architecture with GNN topology ML models is deployed on cloud architecture and evaluated under various criteria. The dynamic ML architecture discovery mechanism is implemented using DNN(GA) on the cloud setup at the research laboratory. The DNN(GA) continuously runs in the background discovering new models for a pre-trained ML model framework bank containing initial candidate ML models. Whenever a new pre-trained model is discovered, it is evaluated against application-specific metrics, and if it outperforms the currently deployed model, it is automatically re-deployed in the cloud environment. The evaluation methodology considerations for the proposed research work include model performance evaluation, runtime overhead, resource and cost utilization during model discovery and convergence, and various fraud dataset experiments to showcase the robustness of the proposed approach across different data distribution. The experiments of the proposed research are implemented in the cloud environment with a credit card fraud detection use case. The cloud infrastructure in the experiments is built on a commercial cloud service provider. The cloud setup consists of a cloud server with a multi-core CPU, single GPU, RAM, disk storage, and network bandwidth, and is used to deploy ML model architecture discovery and fraud detection model training and inference services. The cloud server runs the Linux OS, and the application services are implemented in Python programming language using various libraries and frameworks. The cloud deployment utilizes the Docker containerized environment for ML model deployment and the database. The container orchestration and management tool used in the cloud setup are Kubernetes.

3.1. Data Collection and Preprocessing

The dataset is preprocessed by applying ‘under-sampling’ technique before feeding it to the model for training, testing, and validation. Under-sampling is a technique that involves randomly selecting a set of samples from the majority class and removing the remaining samples from the majority class. Since there are only 492 fraudulent transactions, out of 284,807 total transactions, the dataset is under-sampled by retaining all the fraudulent transactions and only 4,827 genuine transactions. Hence, the final dataset contains 5,319 transactions, out of which 492 are fraudulent and 4,827 are genuine transactions. The dataset is shuffled randomly and split into training, testing, and validation sets in the ratio of 70:20:10.

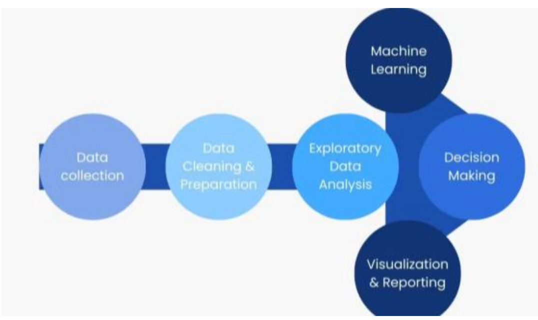

Fig 3 : How data collection & data preprocessing assist machine learning.

To investigate and evaluate the proposed models for detecting fraudulent transactions, a dataset that comprises both genuine and fraudulent transactions is need. Hence, a publicly accessible dataset is retrieved, which contains credit card transactions made in Europe during September 2013. The data includes a total of 284,807 transactions, out of which 492 are confirmed to be fraudulent. Data samples are highly imbalanced; hence, it is difficult to detect fraudulent transactions. Each transaction is described by 30 anonymous numerical features generated by PCA, which transform the features to protect the users' identities and enhance the confidentiality of the data. The only non-anonymous feature is the time, which is recorded in seconds elapsed from the first transaction in the dataset.

3.2. Dynamic Neural Network Architectures

Coherently, the Generative AI technology has received increasing attention recently, along with the rise of ChatGPT and Generative AI applications by leading tech companies. The Generative AI models, trained on immense data, learn latent knowledge and are capable of performing diverse tasks. The Generative AI applications built on Large Language Models (LLMs) have exhibited impressive capabilities in not only NLP-related tasks but also code generation, data analysis, question answering, and even scientific research. To ensure AI audit trails and compliance with industry standards and regulations, there is a high demand for developing ML models in-house rather than relying on black-box third-party AI models. Moreover, the Generative AI models could assist in boosting productivity by providing programming and data analysis support. Overall, there is a compelling and urgent need for financial businesses to develop Real-Time Fraud Detection Systems, leveraging the latest advances in ML and Generative AI technologies.

To cope with the fraud detection and prevention challenge, financial institutions are experiencing the high demand for developing real-time fraud detection systems. By automatically predicting fraud instantaneously after a transaction occurs, fraud detection models can provide businesses with the capability to block fraudulent actions and avoid monetary losses. The wide application of artificial intelligence (AI)-based technologies has made rapid development in machine learning (ML) models for fraud detection.

Equation 3 : Optimization of Neural Network for Real-Time Fraud Detection

$$Q(s_t, a_t) = r_t + \gamma \max_{a'} Q(s_{t+1}, a')$$

Where:

- $Q(s_t, a_t)$ is the expected future reward for detecting fraud based on the state-action pair,
- r_t is the immediate reward (successful fraud detection),
- γ is the discount factor,
- s_{t+1} is the next state.

3.3. Generative AI Techniques

Foundational models are large generative models trained on extensive datasets using self-supervised learning methods. These models can be fine-tuned on specific data to create generative AI applications. Generative modeling employs a generative process to learn data distribution from a training set, enabling the generation of new data points. A generative model can be either explicit, where data probability is directly modeled via density function, or implicit, where data probability is only indirectly modeled.

Generative AI models have exhibited remarkable learning capabilities across diverse domains like language, images, and audio. Recently, researchers have begun harnessing generative AI to simulate complex environments and assist in training novel policies or augmenting the data available for training. Generative AI creates new content based on existing examples, improving exploratory strategies and enhancing the diversity of training scenarios. Generative AI builds on foundational models trained using self-supervised learning on extensive datasets.

4. Experimental Setup

In the wake of the digital transformation, payment systems are moving from cash-based to digital-based. Digital payment systems are widely adopted and preferred as they are convenient, easy to access, and provide lower service cost. The rapid adoption of digital payment systems has raised concerns about online payment frauds. The expansion of online transactions has created opportunities for fraudulent activities. Fraud detection in payment systems is a critical task for financial institutions that incurs high costs. Moreover, misclassifying legitimate transactions as fraudulent causes a loss of business and customer trust. The credit card payment fraud detection system employs multiple models, such as neural networks and observation rules. These models are computationally expensive and may miss the fraudulent transactions during the real-time processing of events or activities. Hence, the new intelligent systems should be developed for the dynamic and adaptive architectures of the neural network models for the real-time fraud detection in the payment systems.

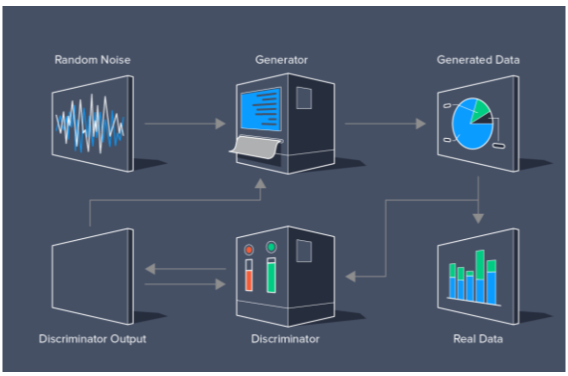

Fig 4 : Generative Adversarial Networks

A generative adversarial network (GAN) model can create new synthetic samples to balance the classes in the credit card transaction dataset. The synthetic samples can be added to the classes with the fewer instances to enhance the performance of the trained ML models. The diversity of the synthetic samples is controlled by a trained critic model using the distance metric. The gradient penalty technique is adopted to regularize the critic model and restrict the slopes of its output concerning the input distance within a range. The models can learn the patterns of the normal transactions during off-line learning. The credit card fraud detection system can classify events as normal or fraudulent transactions based on the trained models from the prior knowledge. The ML models can be dynamically and continually trained with the new data samples to adjust the concepts of the classes. This research effort investigates the dynamic and adaptive architectures of the neural network models for the real-time fraud detection in digital payment systems. The architecture of the fraud detection system involves new events processing using a self-trained multi-class model, creating new classes, and the dynamic training of the new models.

4.1. Dataset Description and Features

Frauds reported typically contain fewer transactions than those conducted, i.e., dozens rather than hundreds or thousands of transactions. This is especially true for more advanced fraud types. In such cases, fraudsters try to go unnoticed and keep frauds below detection thresholds. Overall, transactions are typically subdivided into training (87%), validation (6%), and testing (7%) sets. To analyze model performance on newly emerged fraud types, focus is given on transactions relevant to the fraud type, which are always the least numerous. For each model, two evaluations are therefore conducted based on either all transactions (model generality) or only transactions relating to a specific fraud type (model adaptability).

A detailed analysis of digital payment fraud instances reported to the fraud department of a leading European Bank is presented. All reported instances between 1st April 2019 and 31st March 2021 were documented. Following the Anti Money Laundering (AML) regulations, a similar timeline of transactions is indicated, whereby all transactions relating to a reported fraud were also documented. Each documentation included a set of transaction features. Six features used primarily by fraud analysts were included. Four additional cardholder behavioral features were included. A significant challenge for banks is the non-cooperative fraudsters. New fraud types often emerge that previous banking experience has never encountered. Efforts to investigate such frauds can only begin once a bank has become a victim, i.e., a fraud is reported. Only a snapshot of transactions within a particular fraud type is therefore available.

4.2. Model Training and Evaluation Metrics

The training for each model is accomplished in the Python programming environment using the Keras library with a Tensor Processing Unit (TPU) accelerator on Google Cloud, which ensures faster training times. A batch size of 128 is used for the model training, which also runs for 150 epochs with an early stopping patience of 10 epochs on the validation loss to reduce overfitting. ReLU is used as the activation function for the hidden layers, while Softmax is utilized for the output layer activation function, with categorical cross-entropy identified as the optimal loss function. Furthermore, dropout with a ratio of 0.2 was used as a regularization technique for all hidden layers to mitigate overfitting and maintain model generalization.

Several model evaluation metrics are used to assess the performance of the architecture in predicting credit card fraud, including accuracy, precision, recall, F1-score, and area under the curve score. The detailed mathematical formulas for the evaluation metrics are stated as follows. Accuracy is a measure of how often the model's predictions are correct and is formulated as the fraction of true predictions over all predictions. Precision denotes the ratio of true positives over the predictions made as positive, essentially assessing the model's ability to avoid false positives. Recall signifies the fraction of true positives over all actual positives, depicting the model's sensitivity to the fraudulent class and its ability to minimize false negatives. F1-score is the harmonic mean of precision and recall, offering a way to combine both metrics into one score, especially relevant for imbalanced datasets. AUC score signifies the area under the ROC curve, with the ROC curve plotting the true positive rate against the false positive rate for each class, thus depicting the model's discrimination capability.

5. Results and Discussion

The COVID-19 pandemic is impacting the payments landscape around the world, accelerating the transition towards cashless, contactless, and digital payments. The number of digital payment transactions has almost doubled between 2019 to 2021, resulting in a growth of payment fraud. The number of arrest actions against online fraud has increased by about 60% in 2021. Payment fraud is a high-cost problem for the financial industry. Fraud detection is a classification problem to identify the fraudulent transactions from a pool of valid transactions using historical data for training a classifier. Credit card fraud detection is a well-studied problem with readily available public datasets. Payments fraud or digital payment fraud detection is similar to credit card fraud but differs in terms of the fraudster's profile, payment hierarchy, network, and data characteristics. Data from one payment system cannot be used in another system, and the payment risk models are required to be redeveloped for every new payment system.

Digital payment fraud is a growing concern as financial institutions and retailers are moving to digital payment methods. The need for a fraud mitigation system is required for every digital payment system to monitor transactions in real-time. Various machine learning models can be used to predict fraudulent transactions, but selecting an optimal model, considering accuracy and complexity, is a challenging task. A new approach for developing dynamic neural network architecture using machine learning and generative AI for fraud detection in digital payment systems is proposed. A dynamic deep feedforward neural network model is developed. The model architecture can be configured based on input parameters, and NAS is used to select the optimal architecture. Four different models using diverse training data and architectural configurations are developed. A GAN model using the imbalanced random dataset is developed to generate synthetic samples of the minority class (fraudulent transactions). The proposed architecture and models are evaluated on four different datasets, including benchmark and real-life, low-volume, and high-risk datasets.

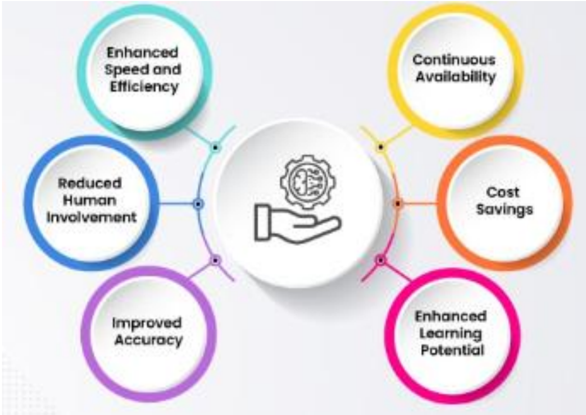

Fig 5 : Understanding AI and ML in Retail Fraud Detection

5.1. Performance Comparison of Different Architectures In order to test the proposed hybrid DL and GL-Filt models, a system architecture was developed in Python programming language using TensorFlow and Keras libraries. In order to characterize the efficiency and potential applicability of the proposed models, the implemented models are compared against 7 other conventional ML and DL models that are widely used in credit card fraud detection: ▪ KNN (K Nearest Neighbors) ▪ RF (Random Forest) ▪ GBC (Gradient Boosted Trees) ▪ DNN (Deep Neural Network) ▪ CNN (Convolutional Neural Network) ▪ LSTM (Long Short-Term Memory) ▪ Auto-Encoder (AE) DNN This section will, hence, discuss the hardware setup, model parameters, evaluation criteria, and the comparison results of the eight models. As to hardware setup, the training and performance comparisons of the implemented models were conducted on a computer with an AMD Ryzen 7 5800H processor, 16 GB of RAM, and an NVIDIA GeForce GTX 1650 with 4 GB of GPU memory. For each model, hyperparameter tuning was performed in order to optimize model performance and avoid over-fitting. The optimized hyperparameters of each model as well as the default values are summarized in Table 2. Regarding evaluation criteria, Accuracy (Acc), F1-score, True Positive Rate (TPR), False Positive Rate (FPR), and Area Under Curve (AUC) score were used to assess model performance. The true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) are determined using the confusion matrix based on the predicted results as listed in Table 3. F1 score represents the degree of system accuracy considering both precision and sensitivity. As the widely used metric for credit card fraud detection, TPR indicates the extent to which actual fraudulent transactions are successfully detected by the system. Meanwhile, FPR indicates the extent to which legitimate transactions are misclassified as fraudulent ones. With points on the x-y plane representing the false positive rate and true positive rate, AUC score quantifies the ability of the model to distinguish between detections and non-detections. A value of 0.5 indicates no distinction, while a value of 1.0 indicates perfect distinction.

5.2. Interpretation of Results

In parallel, an exotic population-based architecture containing a DNN with a novel additive hyper-prior mechanism is proposed to dynamically learn the complexity of the input model architecture. The architecture contains two bio-inspired operation components controlling the number of hidden neurons and hidden layers concerning detection accuracy and model complexity. A comparative analysis was performed between fixed topologies and dynamically evolving topologies of the DNN architecture with additive learning and growth mechanisms to evaluate detection accuracy, run-time performance and model complexity using identical architectural configurations. The outcomes of the experiments indicate that the architecture can learn complex models of fraudulent transactions than fixed topologies while preserving model complexity.An experimental analysis involving ML techniques was performed using an industry-based dataset collected in September 2013 from Europe. A DNN architecture with an auto-encoder technique was developed. The performance of DNN architecture was evaluated concerning detection accuracy and run-time performance while varying the number of neurons in hidden layers as well as the number of hidden layers. To enhance the capability of the DNN architecture to learn complex models of fraudulent transactions, the DNN architecture was developed with a dynamic additive layer neural network-based architecture with a varying number of neurons in hidden layers, fixed at four hidden layer configurations and a fixed learning rate. The influence of the number of hidden layers on learning accuracy was studied at dynamic topologies with a varying number of hidden neurons and hierarchies. The outcomes of this experimentation indicate that with an increase in the number of hidden layers in DNN, the detection accuracy increases and becomes asymptotic at a number of hidden layer configurations higher than four.

6. Conclusion

Future research involves implementing the dynamic neural network architecture development system as a web-based application for DPS PEFs, empowering them to autonomously create novel architectures tailored to specific fraud detection needs. Additionally, investigating advanced techniques for the dynamic architecture refinement's second phase is planned, aiming to minimize the required fraud transaction sample size for architecture refinement.The modern economic landscape necessitates the growth of Digital Payment Systems (DPS), as society transitions towards digitalization. DPS streamlines payment processing, enhances user experiences, and fosters a cashless economy. However, the expanding DPS user base has created opportunities for illicit activities such as hacking and financial frauds. Fraud Detection Systems (FDS) within DPS, empowered by Artificial Intelligence (AI) and Machine Learning (ML), play a crucial role in combating these challenges. Recent advancements in Generative AI, alongside conventional AI and ML techniques, have shown promise in real-time FDS. This work investigates the development of innovative architectures for DPS FDS using Generative AI and ML technologies. A conceptual framework that dynamically develops and refines FDS neural network architectures is proposed. Empirical evaluations demonstrate that the proposed approach meets the requirements of DPS PEFs, significantly enhancing fraud transaction detection rates without compromising genuine transaction acceptance rates.

6.1. Future Directions

The implementation of dynamic neural network architectures for real-time fraud detection in digital payment systems is an innovative and timely solution to an increasingly prevalent issue. Although the current work represents a significant advancement, there are still areas for improvement in terms of performance, effectiveness, and efficiency. One of the major challenges in developing DNNs is determining the network's topology, configurations, and hyper-parameters. This is particularly crucial when creating networks in potentially changing environments, as many pre-defined architectures that perform well in static domains may fail in dynamic application scenarios. One way to address this challenge is through the Automatic Neural Network Architecture Design (ANAAD) proposal, which uses a generative AI agent to automatically design DNN architectures in diverse dynamic environments. In digital payment systems, similar types of DNNs with different architectures can be used for different payment methods. However, other characteristics, such as vigilance, sensitivity, and patience parameters, are carefully selected and fixed, which may not perform well in practice. Future experiments will focus on automatically configuring these parameters for newly generated DNNs. Another aspect that may enhance the current work is the adaptability of tuning mechanisms. In the proof-of-concept implementation, the adaptation mechanisms of ensemble DNNs are switched off after some initial random runs.

References

[1] Laxminarayana Korada. (2023). Role of 5G & Edge Computing in Industry 4.0 Story. International Journal of Communication Networks and Information Security (IJCNIS), 15(3), 366–377. Retrieved from https://www.ijcnis.org/index.php/ijcnis/article/view/7751

[2] Eswar Prasad G, Hemanth Kumar G, Venkata Nagesh B, Manikanth S, Kiran P, et al. (2023) Enhancing Performance of Financial Fraud Detection Through Machine Learning Model. J Contemp Edu Theo Artific Intel: JCETAI-101.

[3] Siddharth K, Gagan Kumar P, Chandrababu K, Janardhana Rao S, Sanjay Ramdas B, et al. (2023) A Comparative Analysis of Network Intrusion Detection Using Different Machine Learning Techniques. J Contemp Edu Theo Artific Intel: JCETAI-102.

[4] Vankayalapati, R. K., Sondinti, L. R., Kalisetty, S., & Valiki, S. (2023). Unifying Edge and Cloud Computing: A Framework for Distributed AI and Real-Time Processing. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i9s(2).3348

[5] Reddy, R. (2023). Predictive Health Insights: Ai And Ml's Frontier In Disease Prevention And Patient Management. Available at SSRN 5038240.

[6] Nampalli, R. C. R. (2023). Moderlizing AI Applications In Ticketing And Reservation Systems: Revolutionizing Passenger Transport Services. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i10s(2).3280

[7] Syed, S. (2023). Shaping The Future Of Large-Scale Vehicle Manufacturing: Planet 2050 Initiatives And The Role Of Predictive Analytics. Nanotechnology Perceptions, 19(3), 103-116.

[8] Korada, L. (2022). Using Digital Twins of a Smart City for Disaster Management. Journal of Computational Analysis and Applications, 30(1).

[9] Janardhana Rao Sunkara, Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Hemanth Kumar Gollangi, et al. (2023) An Evaluation of Medical Image Analysis Using Image Segmentation and Deep Learning Techniques. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-407.DOI: doi.org/10.47363/JAICC/2023(2)388

[10] Kalisetty, S., Pandugula, C., & Mallesham, G. (2023). Leveraging Artificial Intelligence to Enhance Supply Chain Resilience: A Study of Predictive Analytics and Risk Mitigation Strategies. Journal of Artificial Intelligence and Big Data, 3(1), 29–45. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1202

[11] Danda, R. R. Digital Transformation In Agriculture: The Role Of Precision Farming Technologies.

[12] Syed, S. Big Data Analytics In Heavy Vehicle Manufacturing: Advancing Planet 2050 Goals For A Sustainable Automotive Industry.

[13] Gagan Kumar Patra, Chandrababu Kuraku, Siddharth Konkimalla, Venkata Nagesh Boddapati,

Manikanth Sarisa, et al. (2023) Sentiment Analysis of Customer Product Review Based on Machine Learning Techniques in E-Commerce. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-408.DOI: doi.org/10.47363/JAICC/2023(2)38

[14] Sondinti, L. R. K., Kalisetty, S., Polineni, T. N. S., & abhireddy, N. (2023). Towards Quantum-Enhanced Cloud Platforms: Bridging Classical and Quantum Computing for Future Workloads. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i10s(2).3347

[15] Ramanakar Reddy Danda, Z. Y. (2023). Impact of AI-Powered Health Insurance Discounts and Wellness Programs on Member Engagement and Retention. Letters in High Energy Physics.

[16] Syed, S. (2023). Zero Carbon Manufacturing in the Automotive Industry: Integrating Predictive Analytics to Achieve Sustainable Production. Journal of Artificial Intelligence and Big Data, 3, 17-28.

[17] Nagesh Boddapati, V. (2023). AI-Powered Insights: Leveraging Machine Learning And Big Data For Advanced Genomic Research In Healthcare. In Educational Administration: Theory and Practice (pp. 2849–2857). Green Publication. https://doi.org/10.53555/kuey.v29i4.7531

[18] Polineni, T. N. S., abhireddy, N., & Yasmeen, Z. (2023). AI-Powered Predictive Systems for Managing Epidemic Spread in High-Density Populations. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i10s(2).3374

[19] Danda, R. R. (2023). AI-Driven Incentives in Insurance Plans: Transforming Member Health Behavior through Personalized Preventive Care. Letters in High Energy Physics.

[20] Nampalli, R. C. R. (2022). Neural Networks for Enhancing Rail Safety and Security: Real-Time Monitoring and Incident Prediction. In Journal of Artificial Intelligence and Big Data (Vol. 2, Issue 1, pp. 49–63). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2022.1155

[21] Syed, S. (2023). Advanced Manufacturing Analytics: Optimizing Engine Performance through Real-Time Data and Predictive Maintenance. Letters in High Energy Physics, 2023, 184-195.

[22] Patra, G. K., Kuraku, C., Konkimalla, S., Boddapati, V. N., & Sarisa, M. (2023). Voice classification in AI: Harnessing machine learning for enhanced speech recognition. Global Research and Development Journals, 8(12), 19–26. https://doi.org/10.70179/grdjev09i110003

[23] Danda, R. R. (2023). Neural Network-Based Models For Predicting Healthcare Needs In International Travel Coverage Plans.

[24] Subhash Polineni, T. N., Pandugula, C., & Azith Teja Ganti, V. K. (2022). AI-Driven Automation in Monitoring Post-Operative Complications Across Health Systems. Global Journal of Medical Case Reports, 2(1), 1225. Retrieved from https://www.scipublications.com/journal/index.php/gjmcr/article/view/1225

[25] Nampalli, R. C. R. (2022). Machine Learning Applications in Fleet Electrification: Optimizing Vehicle Maintenance and Energy Consumption. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v28i4.8258

[26] Syed, S. (2022). Towards Autonomous Analytics: The Evolution of Self-Service BI Platforms with Machine Learning Integration. In Journal of Artificial Intelligence and Big Data (Vol. 2, Issue 1, pp. 84–96). Science Publications (SCIPUB).https://doi.org/10.31586/jaibd.2022.1157

[27] Sunkara, J. R., Bauskar, S. R., Madhavaram, C. R., Galla, E. P., & Gollangi, H. K. (2023). Optimizing Cloud Computing Performance with Advanced DBMS Techniques: A Comparative Study. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i10s(2).3206

[28] Mandala, G., Danda, R. R., Nishanth, A., Yasmeen, Z., & Maguluri, K. K. AI AND ML IN HEALTHCARE: REDEFINING DIAGNOSTICS, TREATMENT, AND PERSONALIZED MEDICINE.

[29] Kothapalli Sondinti, L. R., & Yasmeen, Z. (2022). Analyzing Behavioral Trends in Credit Card Fraud Patterns: Leveraging Federated Learning and Privacy-Preserving Artificial Intelligence Frameworks. Universal Journal of Business and Management, 2(1), 1224. Retrieved from https://www.scipublications.com/journal/index.php/ujbm/article/view/1224

[30] Rama Chandra Rao Nampalli. (2022). Deep Learning-Based Predictive Models For Rail Signaling And Control Systems: Improving Operational Efficiency And Safety. Migration Letters, 19(6), 1065–

1077. Retrieved from https://migrationletters.com/index.php/ml/article/view/11335
[31] Syed, S. (2022). Integrating Predictive Analytics Into Manufacturing Finance: A Case Study On Cost Control And Zero-Carbon Goals In Automotive Production. Migration Letters, 19(6), 1078-1090.
[32] Rajaram, S. K., Konkimalla, S., Sarisa, M., Gollangi, H. K., Madhavaram, C. R., Reddy, M. S., (2023). AI/ML-Powered Phishing Detection: Building an Impenetrable Email Security System. ISAR Journal of Science and Technology, 1(2), 10-19.
[33] Danda, R. R., Maguluri, K. K., Yasmeen, Z., Mandala, G., & Dileep, V. (2023). Intelligent Healthcare Systems: Harnessing Ai and Ml To Revolutionize Patient Care And Clinical Decision-Making.
[34] Kothapalli Sondinti, L. R., & Syed, S. (2021). The Impact of Instant Credit Card Issuance and Personalized Financial Solutions on Enhancing Customer Experience in the Digital Banking Era. Universal Journal of Finance and Economics, 1(1), 1223. Retrieved from https://www.scipublications.com/journal/index.php/ujfe/article/view/1223
[35] Nampalli, R. C. R. (2021). Leveraging AI in Urban Traffic Management: Addressing Congestion and Traffic Flow with Intelligent Systems. In Journal of Artificial Intelligence and Big Data (Vol. 1, Issue 1, pp. 86–99). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2021.1151
[36] Syed, S. (2021). Financial Implications of Predictive Analytics in Vehicle Manufacturing: Insights for Budget Optimization and Resource Allocation. Journal of Artificial Intelligence and Big Data, 1(1), 111–125. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1154
[37] Patra, G. K., Rajaram, S. K., Boddapati, V. N., Kuraku, C., & Gollangi, H. K. (2022). Advancing Digital Payment Systems: Combining AI, Big Data, and Biometric Authentication for Enhanced Security. International Journal of Engineering and Computer Science, 11(08), 25618–25631. https://doi.org/10.18535/ijecs/v11i08.4698
[38] Danda, R. R. Decision-Making in Medicare Prescription Drug Plans: A Generative AI Approach to Consumer Behavior Analysis.
[39] Vankayalapati, R. K., Edward, A., & Yasmeen, Z. (2022). Composable Infrastructure: Towards Dynamic Resource Allocation in Multi-Cloud Environments. Universal Journal of Computer Sciences and Communications, 1(1), 1222. Retrieved from https://www.scipublications.com/journal/index.php/ujcsc/article/view/1222
[40] Syed, S., & Nampalli, R. C. R. (2021). Empowering Users: The Role Of AI In Enhancing Self-Service BI For Data-Driven Decision Making. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v27i4.8105
[41] Sarisa, M., Boddapati, V. N., Kumar Patra, G., Kuraku, C., & Konkimalla, S. (2022). Deep Learning Approaches To Image Classification: Exploring The Future Of Visual Data Analysis. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v28i4.7863
[42] Danda, R. R. (2022). Application of Neural Networks in Optimizing Health Outcomes in Medicare Advantage and Supplement Plans. Journal of Artificial Intelligence and Big Data, 2(1), 97–111. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1178
[43] Syed, S., & Nampalli, R. C. R. (2020). Data Lineage Strategies – A Modernized View. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v26i4.8104
[44] Sondinti, L. R. K., & Yasmeen, Z. (2022). Analyzing Behavioral Trends in Credit Card Fraud Patterns: Leveraging Federated Learning and Privacy-Preserving Artificial Intelligence Frameworks.
[45] Syed, S. (2019). Roadmap for Enterprise Information Management: Strategies and Approaches in 2019. International Journal of Engineering and Computer Science, 8(12), 24907–24917. https://doi.org/10.18535/ijecs/v8i12.4415
[46] Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., & Gollangi, H. K. (2022). PREDICTING DISEASE OUTBREAKS USING AI AND BIG DATA: A NEW FRONTIER IN HEALTHCARE ANALYTICS. In European Chemical Bulletin. Green Publication. https://doi.org/10.53555/ecb.v11:i12.17745
[47] Danda, R. R. (2022). Deep Learning Approaches For Cost-Benefit Analysis Of Vision And Dental Coverage In Comprehensive Health Plans. Migration Letters, 19(6), 1103-1118.
[48] Maguluri, K. K., Yasmeen, Z., & Nampalli, R. C. R. (2022). Big Data Solutions For Mapping Genetic Markers Associated With Lifestyle Diseases. Migration Letters, 19(6), 1188-1204.

[49] Eswar Prasad Galla.et.al. (2021). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions Educational Administration: Theory and Practice, 27(4), 1228 –1236Doi: 10.53555/kuey.v27i4.7592

[50] Ramanakar Reddy Danda. (2022). Telehealth In Medicare Plans: Leveraging AI For Improved Accessibility And Senior Care Quality. Migration Letters, 19(6), 1133–1143. Retrieved from https://migrationletters.com/index.php/ml/article/view/11446

[51] Vankayalapati, R. K., & Syed, S. (2020). Green Cloud Computing: Strategies for Building Sustainable Data Center Ecosystems. Online Journal of Engineering Sciences, 1(1), 1229. Retrieved from https://www.scipublications.com/journal/index.php/ojes/article/view/1229

[52] Venkata Nagesh Boddapati, Eswar Prasad Galla, Janardhana Rao Sunkara, Sanjay Ramdas Bauskar, Gagan Kumar Patra, Chandrababu Kuraku, Chandrakanth Rao Madhavaram, 2021. "Harnessing the Power of Big Data: The Evolution of AI and Machine Learning in Modern Times", ESP Journal of Engineering & Technology Advancements, 1(2): 134-146.

[53] Danda, R. R. (2020). Predictive Modeling with AI and ML for Small Business Health Plans: Improving Employee Health Outcomes and Reducing Costs. In International Journal of Engineering and Computer Science (Vol. 9, Issue 12, pp. 25275–25288). Valley International. https://doi.org/10.18535/ijecs/v9i12.4572

[54] Vankayalapati, R. K., & Rao Nampalli, R. C. (2019). Explainable Analytics in Multi-Cloud Environments: A Framework for Transparent Decision-Making. Journal of Artificial Intelligence and Big Data, 1(1), 1228. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1228

[55] Mohit Surender Reddy, Manikanth Sarisa, Siddharth Konkimalla, Sanjay Ramdas Bauskar, Hemanth Kumar Gollangi, Eswar Prasad Galla, Shravan Kumar Rajaram, 2021. "Predicting tomorrow's Ailments: How AI/ML Is Transforming Disease Forecasting", ESP Journal of Engineering & Technology Advancements, 1(2): 188-200.

[56] Ganti, V. K. A. T., & Pandugula, C. Tulasi Naga Subhash Polineni, Goli Mallesham (2023) Exploring the Intersection of Bioethics and AI-Driven Clinical Decision-Making: Navigating the Ethical Challenges of Deep Learning Applications in Personalized Medicine and Experimental Treatments. Journal of Material Sciences & Manufacturing Research. SRC/JMSMR-230. DOI: doi. org/10.47363/JMSMR/2023 (4), 192, 1-10.

[57] Chandrakanth R. M., Eswar P. G., Mohit S. R., Manikanth S., Venkata N. B., & Siddharth K. (2021). Predicting Diabetes Mellitus in Healthcare: A Comparative Analysis of Machine Learning Algorithms on Big Dataset. In Global Journal of Research in Engineering & Computer Sciences (Vol. 1, Number 1, pp. 1–11). https://doi.org/10.5281/zenodo.14010835

[58] Sondinti, L. R. K., & Syed, S. (2022). The Impact of Instant Credit Card Issuance and Personalized Financial Solutions on Enhancing Customer Experience in the Digital Banking Era. Finance and Economics, 1(1), 1223.

[59] Vaka, D. K. (2023). Achieving Digital Excellence In Supply Chain Through Advanced Technologies. Educational Administration: Theory and Practice, 29(4), 680-688.

[60] Sarisa, M., Boddapati, V. N., Patra, G. K., Kuraku, C., Konkimalla, S., & Rajaram, S. K. (2020). An Effective Predicting E-Commerce Sales & Management System Based on Machine Learning Methods. Journal of Artificial Intelligence and Big Data, 1(1), 75–85. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1110

[61] Vaka, D. K. Empowering Food and Beverage Businesses with S/4HANA: Addressing Challenges Effectively. J Artif Intell Mach Learn & Data Sci 2023, 1(2), 376-381.

[62] Gollangi, H. K., Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., & Reddy, M. S. (2020). Exploring AI Algorithms for Cancer Classification and Prediction Using Electronic Health Records. Journal of Artificial Intelligence and Big Data, 1(1), 65–74. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1109

[63] Vaka, D. K. "Artificial intelligence enabled Demand Sensing: Enhancing Supply Chain Responsiveness.

[64] Manikanth Sarisa, Venkata Nagesh Boddapati, Gagan Kumar Patra, Chandrababu Kuraku, Siddharth Konkimalla, Shravan Kumar Rajaram.Navigating the Complexities of Cyber Threats, Sentiment, and

Health with AI/ML. (2020). JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 8(2), 22-40. https://doi.org/10.70589/JRTCSE.2020.2.3

[65] Vaka, D. K. (2020). Navigating Uncertainty: The Power of ‘Just in Time SAP for Supply Chain Dynamics. Journal of Technological Innovations, 1(2).

[66] Gollangi, H. K., Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., & Reddy, M. S. (2020).Unveiling the Hidden Patterns: AI-Driven Innovations in Image Processing and Acoustic Signal Detection. (2020). JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 8(1), 25-45. https://doi.org/10.70589/JRTCSE.2020.1.3.

[67] Dilip Kumar Vaka. (2019). Cloud-Driven Excellence: A Comprehensive Evaluation of SAP S/4HANA ERP. Journal of Scientific and Engineering Research. https://doi.org/10.5281/ZENODO.11219959

[68] Hemanth Kumar Gollangi, Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Janardhana Rao Sunkara and Mohit Surender Reddy.(2020). “Echoes in Pixels: The intersection of Image Processing and Sound detection through the lens of AI and Ml”, International Journal of Development Research. 10,(08),39735-39743. https://doi.org/10.37118/ijdr.28839.28.2020.

[69] Manikanth Sarisa, Venkata Nagesh Boddapati, Gagan Kumar Patra, Chandrababu Kuraku, Siddharth Konkimalla and Shravan Kumar Rajaram. “The power of sentiment: big data analytics meets machine learning for emotional insights”, International Journal of Development Research, 10, (10), 41565-41573.