Journal of Artificial Intelligence and Big Data Disciplines (JAIBDD)

International | Peer Reviewed | Open Access | Online

Deep Learning Architectures for Automated Fraud Detection in Payroll and Financial Management Services: Towards Safer Small Business Transactions

Jeevani Singireddy
Sr.Software Engineer, Intuit Inc.,
Temecula,CA

Abstract : Fraudulent payroll accounts are a significant issue in the financial and payroll services market. About 75 percent of employees have stolen from their employer once, 20 percent have stolen at least twice, and half of this figure has stolen at least three times or more. The increased use of direct deposit has made it easier to steal the identity of a small payroll customer. A fraudulent account is set up with apparently legitimate credentials, and the account's data set is changed after the customer's login authentication returns an all-is-ok status. The direct deposits are then quickly withdrawn. It's an ongoing game of cat-and-mouse: after a bank improves or alters its fraud detection system, criminals quickly adapt to avoid it. Small-scale business contract fraud is accepted and paid as normal business expenses, and there is extremely little fraud detection technology in place to pick up the kickback schemes. This type of fraud can bring a company to its knees. (B) Automated fraud detection in payroll and financial management services harnesses sophisticated deep learning architectures. Computers do the heavy lifting for identifying patterns, obtaining insights, making decisions, and taking action. Unless large fraudulent datasets are already commercially available, the models are unable to understand or predict fraud when trained only on legitimate transaction data. Constructing artificially oversampled imbalanced data sets leads to flawed models. A self-training active learning ensemble stack of models using transaction authentication data is described. It directly leverages fraud patterns in a mostly-unlabeled data set and requires minimal retraining when a pattern changes. Model performance is measured with area under the ROC curve, and this method outperforms existing techniques.

Keywords: Data sharing, fraud and anomaly detection, payroll, small business, privacy preservation, collaborative DL, financial services.

1. Introduction

Automated fraud detection systems play a significant role in ensuring that payroll and financial management transactions are safe. This paper presents a concise study of the latest Deep Learning (DL) architectures that are specifically utilized for automated detection of monetary deception in companies providing payroll and financial management services. The curated DL models are based on their architecture, methods, the technical details of how they were used in the original study, the dataset employed there, and their primary results. In general, the financial industry is vulnerable to fraud threats and their impact can be huge, particularly for small businesses. This study aims to inform and empower transaction processors, payment processors, or payment service providers, legally responsible for conducting automated transactions of small businesses. Providing assistance to supervise, identify, and deter deliberate deception in-house and out-house financial transactions may be of strategic value to these stakeholders.

Digital transaction processing is widely applied in small businesses to facilitate payroll and financial management transactions. For instance, retail businesses may process a large number of sales transactions daily, for which payment processors are employed to handle credit card and debit card payments. Similarly, payroll processors can be used to dole out workers' wages as flat-rate or hourly transactions. The digital sector is the pioneering industrial sector in exploiting digitized financial transactions. Therefore, COVID-19 resulted in fraud in this industry, which led to a sudden spike in its implications.

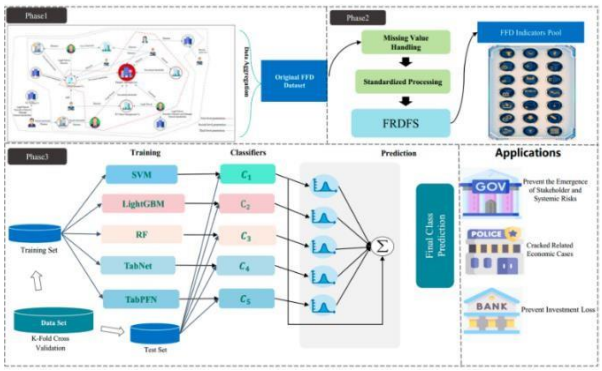

Fig 1: Financial Fraud Detection

1.1 Background and Significance of Fraud Detection in Payroll and Financial Management Services

Fraudulent transactions and how to detect them remain a significant problem for financial institutions around the world. Fraud comes with a high cost for financial organizations, damaging the financial well-being and trust of a financial organization's users. Small and medium enterprises (SMEs) are particularly vulnerable. SMEs account for 99.9% of the country's enterprises and represent 60% of the private sector. Given their significant presence in the economy, up to 58% of small businesses experience financial fraud in a specified period. A common form of this fraud comes in the form of "social attacks," where scammers use deceit and manipulation to trick targeted employees into making illegal payments, accessing sensitive information, or updating account details, among other things. Although large financial organizations could possess the instrumental capacity to identify and prevent fraud, in the case of SMEs, the risk of exploitation of such schemes undermines their ability to recognize fraud attempts and take preventive measures, which can occasionally lead to significant financial losses. To alleviate this situation and protect these vital entities, there is a pressing need for the development of high-performance automated fraud detection solutions, tailored to SMEs using modern deep learning algorithms.

Equation 1: Model Architecture (Neural Network Layers)

$$\mathbf{h}^{(l)} = \sigma\left(\mathbf{W}^{(l)}\mathbf{h}^{(l-1)} + \mathbf{b}^{(l)}\right)$$

Where:

- $\mathbf{h}^{(l)}$ is the activation of the l-th layer,
- $\mathbf{W}^{(l)}$ is the weight matrix for the l-th layer,
- $\mathbf{b}^{(l)}$ is the bias vector for the l-th layer,
- $\sigma(\cdot)$ is the activation function (e.g., ReLU, Sigmoid, or Tanh).

2. Literature Review

In this Section current and related work in the area of online financial fraud detection are reviewed. As financial transactions increase rapidly, online financial fraud has become an important part of internet crime. There are a variety of ways in which online financial fraud is committed. The structure containing these elements (financial transactions, fraud types, features, ML algorithms and performance metrics) comprises a hybrid form of the systems used in the reviewed works. The mentioned and reviewed algorithms: Logistic Regression, Random Forest, decision tree, SVM and Neural Network are the most commonly used for detecting online financial fraud. In recent years, many works have been published on the topic of online fraud detection. There have been many methods proposed in the literature to accurately detect online financial fraud, but the issue requires remarkable improvement in order to predict online financial fraud more accurately.

In recent years, online financial fraud has been observed increasing, ranging from credit card fraud to account takeover fraud. To fight against sophisticated evildoers operating in the form of organized crime, fraud teams are being established. The main mission is to address fraudulent charges becoming the hardest category to detect and the category that brings along most false positives. Although under immense pressure from regulators and card associations, there is an absence of guidance particularly on model selection, validation, and evaluation, a unified metric, and how to signal to the regulator that the organization has done enough. Moreover, not much academic work is devoted to studying the detection of fraudulent charges.

2.1. Traditional Methods of Fraud Detection in Payroll and Financial Management Services

Fraud have existed for a long time, long before computers, bank cards, and other technologies. The ‘modern’ face of fraud is not different from the old one, except that it is perpetrated over the internet. The growth in new technology has multiplied the avenues through which fraudulent behavior can be perpetrated. A foundational approach to studying fraudulent behavior is the ‘fraud triangle’. Cressey emphasized the elements that must be present for fraud to occur. For fraud to manifest within a set of circumstances, three key elements must be present: the first is the incentive or pressure, the second is the opportunity, and the third is the rationalization by the perpetrator.

Irrespective of channel type, financial institutions are faced with combating a staggering volume of fraudulent transactions. In the context of credit transactions, for instance, criminals have seemingly unlimited patience to reconstruct a client's credit card and siphon off funds. In recognition of this, finance regulators have exhorted businesses to consider innovative solutions that are rooted in machine learning to help detect and mitigate fraud. Machine learning is a method that blends computer algorithms with statistical modeling, enabling computer systems to learn from training data. These systems can then be used to predict the outputs of new data. Recently, deep learning methods have been shown to produce state-of-the-art results over conventional machine learning methods in many domains. Deep learning is a form of machine learning involving artificial neural networks that can be utilized to decipher the intricate relationships in data. In the context of fraud detection, this can mean detecting fraudulent behavior from billions of legitimate transactions, which can be likened to finding a needle in a haystack. Various machine learning and deep learning approaches have thus far been explored to assist in the early identification of deceitful behavior to help minimize the risk of business catastrophic loss.

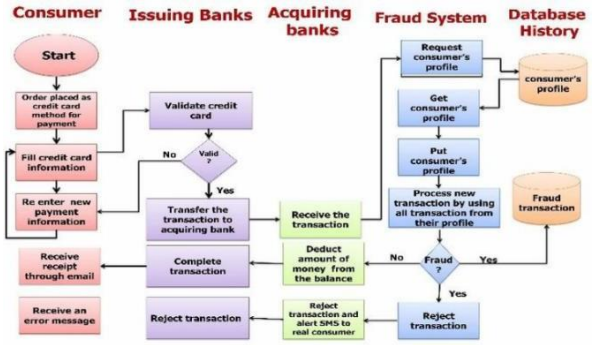

Fig 2: Traditional Methods of Fraud Detection

2.2. Advancements in Deep Learning for Fraud Detection

Fraud can be greatly reduced if detected timely, which has made fraud detection an important research field in recent years. With the development of artificial intelligence and machine learning, a variety of new methods for fraud detection have emerged, providing a new approach for fraud detection research. Fraud detection can generally be seen as a classification problem, while the predictors are usually built by supervised machine learning algorithms currently. In order to improve the performance of fraud detection, different prediction models have been proposed in the past, and it has been found that the prediction model has a great influence on the fraud detection performance. Deep learning based on neural networks has received widespread attention due to its excellent performance in various fields. On the other hand, fraud detection research is often presented as a classification issue, while the research object of deep learning is how to accurately represent the data. Deep learning can encapsulate complex features in the data and make predictions based on them.

Currently, there is no in-depth discussion in the literature on how to choose from conventional machine learning methods and deep learning to design the prediction model for fraud detection. The trade-off between conventional methods and deep learning mainly focuses on the interpretability of the model, the generalization of the data representation, and the availability of the data. Although many conventional machine learning methods have a good interpretability, they usually can't represent the data well enough compared with deep learning. On the other hand, many deep learning models are over complex, and it is difficult to understand the implicit logic behind them. Besides, modeling with deep learning requires a large amount of training samples, while these samples are often difficult to obtain in real problems. There is currently no in-depth discussion on addressing the unbalance between detection rates and false positive rates in the detection results. This is because the selection of indicators to evaluate the predicted results is often arbitrary and is not necessarily appropriate. For instance, it is observed that the AUC value is more than 0.99 when the probability threshold is very high in the ROC curve, although this model is difficult to evaluate. If the fraud detection model assesses the detection results based on a certain level of FP rate (e.g., 1%), it is found that the TDP and BDT models have the best TPR performance while maintaining an acceptable level of FPR performance.

3. Theoretical Foundations of Deep Learning

This section introduces fundamental machine learning and privacy principles relevant to readers unfamiliar with the domains outlined in the introduction. It also discusses standard definitions in differential privacy literature, together with a summary of relevant work on privacy-aware machine learning and fraud detection systems. Lastly, this part covers technical background concerning sequence-to-sequence learning with integrated side modules, which is elucidated utilising Transformers. Transformation mechanisms applied to token level inputs (featuring attribution values) are detailed, as well as the attention-based aggregation of token level embeddings to input data sequences.

Innovation in machine learning (ML) methodologies and data availability over the last years has meant substantial advances to provision financial system actors with tools for fraud prevention and anti-money laundering. Such services are an industry on their own, with Financial Institutions contracting a broad ecosystem of technology partners and risk management vendors. The latter take the form of either standalone tools or 'black box' service providers offering analytics platforms interconnected with retail and investment banks, asset managers, and central banks. In recent years, due to breaches recorded by the Financial Conduct Authority. Many high-street UK banks have temporarily shut down payment services and accounts linked to cryptocurrency exchange platforms. Central banks and governmental bodies recognise the limitations of isolated tools when combating systemic risks and are now concerned with the development of incentives for financial data sharing. The information leakage of data-centric algorithms is unaccounted for by current evaluations, and usually neglected in the FS industry. Thus, members of select US Senate committees appealed to the Government

Accountability Office. In response, federal agencies commit to explore collaborative ML approaches beyond conventional data sharing analyses. Major institutions are found to benefit from improved predictive capabilities using hybrid processes that federate Deep Learning (DL) architectures in fraud prevention. Complex sequential data streams are prevalent within financial institutions and, as such, many of the latter DL models are informed or consume data on a token level. On an input sequence of transactions, these models learn to detect deviations from an individual or account-dependent pattern in the data. Similarly to the time a financial transaction is logged, account holders are notified via push notification and application interfaces of … as well as the details disclosed on the account balance. The former class of data is a cause of insensitivity and curtailment of personal expense patterns, and its consultation to model design and feature selection risks.

3.1. Neural Networks and Deep Learning Basics

In recent years, deep learning is becoming an increasingly attractive research field with a wide range of applications for data mining tasks. Deep learning emphasizes representation learning through multiple layers of non-linear transformation and typically refers to neural networks with many hidden layers, which is rooted in models like artificial neural networks and their broad generalizations. Deep learning architecture has been widely applied in a variety of fields, showing significant advantages in various domains. Different from ML and shallow NN, DL can learn features directly from the input data, needing no manual or preset feature extraction. Source data can be raw or a low level view, greatly reducing human cost. The mining procedure can be more iteratively updated and adjusted due to flexible network structures. Overall DL can be deemed as an end-to-end data-driven method. However, DL is not suitable for all problems and domains. Payroll providers manage the generation and distribution of pay for employees in the businesses that cannot support a full-time payroll employee. The growth of small businesses has led to increased transaction risk, as most transactions are now made via online payments. The owner of a small business can be the same person responsible for the payroll. If struck by fraud, money deposited into the business account can be stolen, resulting in empty payrolls and bounced checks. Detecting payroll fraud in the earliest stages is crucial. Through this thesis, the author explores the impact of implementing DL architecture on emerging small business services and the potential for early detection of fraud in transactions. Small businesses often rely more on online payment services due to the speed of service and it is impossible to handle many customers. However, if a business strike is defrauded, it is likely that money deposited into the account will be immediately withdrawn and payrolls will not be paid on the agreed date. As a result, a manager may be forced to write checks or otherwise compensate for the deduction. Owners or managers can also be distracted between payroll activities and business operations, opening opportunities for employees to take advantage.

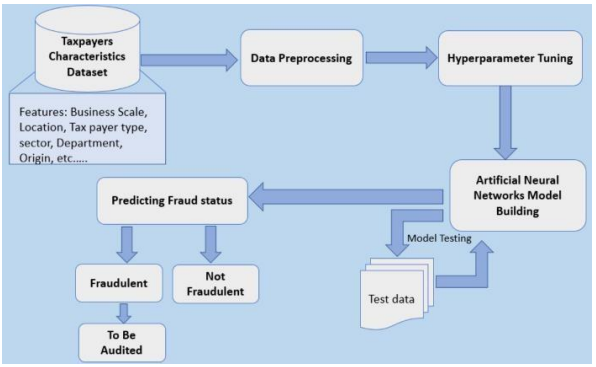

Fig 3: Fraud Detection Using Neural Networks

3.2. Convolutional Neural Networks (CNNs)

Fu, Principe, and Lee solved a problem in detecting card fraud by training the architecture of the LeNet-5 convolutional neural network. To train LeNet-5, transactions in feature form were presented in the form of sliding one-dimensional signals. The results showed the superiority of LeNet-5 over several algorithms: the Support Vector Machine, the Artificial Neural Network, and the Random Forest. By thinning the one-dimensional display of the input, the original data are utilized more efficiently and a more stable classification is initiated. The architecture of LeNet-5 is adjusted to suit the characteristics of financial transaction data, and the algorithm is proposed for the company's fraud detection software. It is designed to be used for this task, a model for a series of connected layers such that each layer of the feature map by means of a sequence of convolutional and a pooling operation. The model is trained to update the detection system. Heryadi and Warnars have tried to combine CNN with a recurrent LSTM network to detect fraud. For this, a hybrid architecture of a CNN-LSTM network is developed with the aim of transforming transaction data into financial feature maps. However, it is shown that the simple CNN architecture is already better equipped to detect fraud compared to the developed CNN-LSTM architecture. Furthermore, a fraud dataset is analyzed to look at the length of the fraud scheme

Equation 2: Fraud Detection Output (Classification Layer)

$$y_{\text{pred}} = \sigma\left(\mathbf{W}^{(L)}\mathbf{h}^{(L-1)} + \mathbf{b}^{(L)}\right)$$

Where:

- y_{pred} is the predicted probability of fraud,
- L is the number of layers in the model.

4. Deep Learning Architectures for Fraud Detection

Despite the fact that nearly 9,000 payroll and financial management firms serve nearly 5 million small businesses with reasonable accuracy, the market is plagued by fraudulent transactions executed by insiders, such as embezzlement schemes that cause substantial financial losses, render identity protection measures employed for personal transactions inert, tarnish the affected parties' credit ratings, and significantly impair the reputation of all stakeholders. An automatic fraud detection system designed to defend the interests of the legitimate stakeholders of the industry and the general public is absent from research and commercial production. While studies conducted on the implementation of automated payroll transactions help safeguard data integrity and transactional behavior, there is no system that monitors and evaluates the appropriateness of human modifications of financial data that contain opportunities for embezzlement. In this study, we contribute to a deeper understanding of how to design effective deep learning models to detect potentially fraudulent bank transactions appearing on bank reconciliations, an externally generated report that reconciles differences between the employer's general ledger and the payroll service bureau's detailed books. With this information, payroll or financial management firms can jumpstart their fraud detection programs and take corrective actions with relevant human resources and the affected parties.

In this section, deep learning is applied to the study of automated fraud detection for the enterprise data set that is described in the following sections. The data dictionary is given in a subsequent section, while the classification results of our deep learning algorithms are described in another section. Actually, deep learning models have been developed with bias-corrected logistic regressions operating as input gates that generate predicted probabilities that guide external validity tests of internal audit functions staffed by professionals with different skill sets and resource constraints

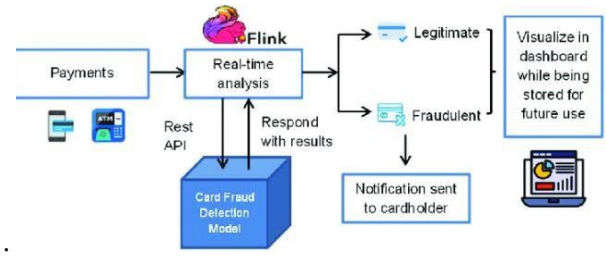

Fig 4: Fraud detection architecture

4.1. Deep Neural Networks (DNNs)

Due to the complexity and importance of the global financial system, safeguarding fraud vulnerabilities within has become top priority for financial security. Therefore, deep learning architectures for effectively detecting and preventing various types of frauds in payroll and financial management services is imperative for maintaining smooth and secure small business transactions. Current deep learning based automated fraud detection research studies conduct text mining or model based solutions with a particular focus on underlying spatial or statistical properties of the data. This study pushes the frontier of deep learning based fraud detection research in payroll and financial management services by rigorously investigating the task of safeguarding small businesses against fraudsters via space-time deep learning frameworks designed based on spatial-temporal properties of transactions, frauds, and businesses.

- This approach is implemented by introducing innovative deep learning architectures that leverage state-of-the-art deep neural networks, Long-Short Term Memory and time-distributed dense layers, on stream-based structured sequential data over the transaction/fraud period of businesses. Furthermore, it is possible to design and implement efficient computation network structures composed of feedforward DNNs.

- In particular, it is proposed a DNN based framework for first generating embedded transaction-features that are time distributed across transaction streams of businesses to recurrent or convolutional networks for detecting fraud behaviors, based on only a set of features in a transaction. To verify the robustness and effectiveness of various proposed deep learning architectures, intensive experiments are conducted on real-world large-scale payroll transactions and small businesses. Empirically, it is justified that the proposed deep learning architectures can accomplish the effect of fraud detection in an efficient and effective way, and they outperform various types of extensive fraud detection models from a wide range of baselines using text mining and standard machine learning approaches.

4.2. Long Short-Term Memory Networks (LSTMs)

In the field of electronic finance, due to the growing use of the Internet and smart devices, more financial transactions and behaviors have been transferred to the network and digitized. Traditional financial fraud detection methods chiefly use the features related to credit activities of clients, such as returned checks, type of cards, amount of money, etc. However, financial transactional data is generating intricate and unstructured behavioral data describing humans' interactions with websites, watching online streaming videos, apps, and other smart devices or sensors. These behavioral data need to be efficiently pre-processed in order to benefit from a variety of machine learning approaches. Special attention was conducted on the design of recurrent neural network (RNN) based deep learning network architectures to efficiently process unstructured sequential behaviors. A deep-learning approach, RNN with different types of network architectures, was proposed to predict online fraud behaviors based on a customer's interactions with websites or smart-phone applications as a sequence of states. This sequence of behaviors are generated by a customer at all time points if a transfer was made. Behavior number grouping keeps incrementing if it is the same as the previous time points and returns back to '1' if subsequent behaviors change. Behaviors are represented through behavior numbers and stay in this form until a next transfer happens.

5. Data Preprocessing and Feature Engineering

As a market for goods, services, and information becomes progressively digital, so too do the transactions that mediate this exchange. Cash transactions have declined in favor of digital and card-based payment methods. Similarly, in exploratory interviews conducted with several leading small business transaction processing companies, it was found that a larger proportion of their mid-to-large sized vendors increasingly choose to take payment via digital platforms. This is a mismatch with enterprise-centered fraud detection strategies utilized by this vertical. Larger businesses utilize dedicated payroll and financial management services, which are well-integrated with their IT infrastructure, and use enterprise-centered fraud filter services. Despite these tools, in 2018 the American payroll company reported that the most common form of fraud was the impersonation of a company officer, typically to transfer payroll out of the company pocket. There is a market opportunity for small business transaction processing companies to pivot to services that better protect their vendors.

To harness the value in unstructured and semi-structured data, data preprocessing and feature engineering are vital components of analysis pipelines for machine learning complex algorithms. Transforming datasets from a raw form with missing data points, outliers, and noise to a structured form with interpretable features is a fundamental challenge in applied data science. As with all data science tasks, the quality of data going into the model directly influences the performance and quality of the results. Varied data preprocessing techniques are therefore applied to prepare the datasets properly for analysis. On small datasets, an algorithm can be fitted and tested relatively quickly to gauge what data and features should be prioritized; however, for large datasets, a strategy is necessary to navigate the computational difficulties that manifest from training each model. While exact best practices are still the subject of debate, there are several guidelines that can be followed to prepare a "clean" dataset which is then ready for the application of an algorithm.

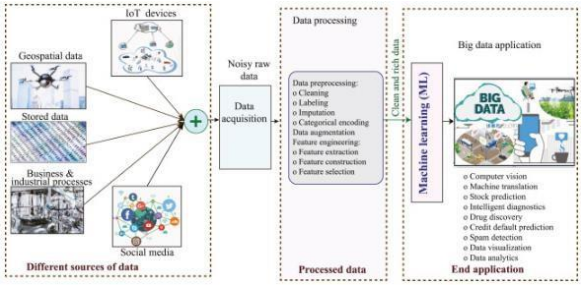

Fig 5: Data processing and feature engineering

5.1. Data Cleaning and Transformation

Financial services are a highly vulnerable sector for fraudulent activities. Since businesses usually operate and pay to employees via banks/financial entities, there is an opportunity to use bank-based financial management services for detecting fraud. Market statistics show that small businesses suffer from the majority of fraudulent activities. Thus, detecting fraud in financial services would particularly benefit small businesses. Reviewed is existing literature on fraud detection in banking systems, which has spurred the development of a novel deep learning architecture for automatically detecting fraud, to be validated using a quarter-million transaction dataset from a payroll and financial management services company.

The effectiveness of the new architecture is validated using a large-scale, real-world transaction dataset obtained from a payroll and financial management services company. The dataset contains around 0.25 million transactions of a small enterprise that has been operating since 2016. The data was collected in a period of 2 years and includes timestamps, recipients, total payment amount, and exchanged goods/services. The enterprise is located in a Nordic country and makes money transactions via a digital payment platform supported by a fintech actor.

5.2. Feature Selection and Extraction

Fraud detection is a critically important process for many businesses and financial institutions. Analyzing financial transactions in an attempt to identify questionable activity is a standard means for determining evidence of fraud. Although automation is increasingly common in this area, it is usually only adopted by large institutions with access to very large datasets and computational resources. Therefore, a generalized and scalable method which is useful for smaller businesses is presented and evaluated. It is predicated on the characteristics of two classes of financial fraud cases: payroll and financial statement fraud. The method uses historical databases of filed court cases to construct large datasets which can be sliced and diced along multiple dimensions, allowing for the training of various deep learning architectures.

Ultimately, the learned models are accurate and optimal, achieving an average true positive rate of over 0.85 and an average F1 score of over 0.63. Deep learning architectures have gained prominence in fraud detection research in recent years. They offer a scalable, automatic means of learning feature representations, and can be very effective given large datasets. All deep learning applications to fraud detection tasks this study has a great disparity between the number of interests. Only those large datasets for which solid results have been achieved are included. The majority of small business owners involved in financial fraud cases are charged under federal counts of "Theft or Embezzlement Concerning Programs Receiving Federal Funds" or "Mail Fraud". Case descriptions do not provide sufficient information to recover detailed financial data, only a general narrative of each crime.

Equation 3: Loss Function

$$\mathcal{L} = -\frac{1}{m}\sum_{i=1}^{m}\left(y_{\text{true}}^{(i)}\log(y_{\text{pred}}^{(i)}) + (1-y_{\text{true}}^{(i)})\log(1-y_{\text{pred}}^{(i)})\right)$$

Where:

- m is the number of transactions in the batch,
- $y_{\text{true}}^{(i)}$ is the true label for the i-th transaction,
- $y_{\text{pred}}^{(i)}$ is the predicted probability for the i-th transaction.

6. Conclusion and Recommendations

With the particularly advanced technology of artificial intelligence (AI), a specific source known as deep learning from a collection of AI methods that can recognize patterns automatically from data may become particularly associated, and an increasing research topic, because of its high productivity examining modern research progress. The acceleration of development is particularly motivated as a consequence of advanced robotization, digital transformation, and big data development. Firms in various fields are expected to be able to use deep learning techniques to extract knowledge from perspective and historical data which will then be commonly utilized to serve as the basis for analytics, productivity improvement, and effectiveness. Particularly small-to-medium-sized businesses (SMBs) and enterprises appear to be well-known for sharing difficult conditions and always under-optimization. The implementation of deep learning is generally complex because the development requirements for expertise and specialized systems are significant. Based on the Customer Unlabelled Sequence, Two Stream Recurrent Neural Network was defined explicitly for payroll transaction unlabelled sequence anomaly discovery [7]. Thus, the company, consultants, and software developers may effectively generate proposals, software, and systems based on market requests through the research project and conference. Software developers can easily launch enterprises in payroll and financial executive services and offer secure payment administration services. For choices and trade strategy, SMEs and payments experts can obtain valuable information and advice. Small enterprises and potential payments suppliers, as the business demand for deep learning in transaction fraud detection and corporate advisory transactions is known, can initiate changes in response to known patterns utilizing existing and readily available storage and enterprise productivity tools to limit financial fraud.

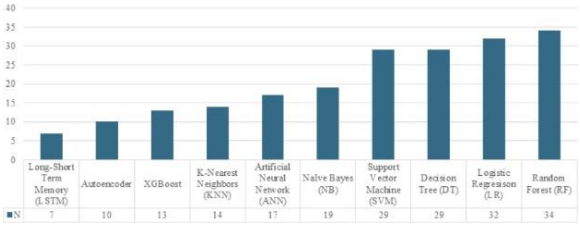

Fig : Financial fraud detection

6.1. Summary of Key Findings

NewRealm, a financial consulting firm, realized the potential in offering clients the benefits of both specialized financial management advice and Local Blend payroll services. After recruiting seasoned professionals with expertise in financial management services, NewRealm introduced hundreds of small local business clients to the program that originated as a pilot project. The account managers visit the businesses periodically, providing support and ensuring high client retention rates thanks to this relationship. In time, this client partnership led to rapid growth and financial success for NewRealm, which transitioned from a boutique provider to a national firm serving large organizations. While Local Blend preserved that personal customer service approach, NewRealm took advantage of its comprehensive consulting capabilities, with automated systems created for their large client base that also monitors for signs of financial crime. Therefore, Local Blend became a vessel to illicitly transfer funds from the large corporations that NewRealm serviced, targeting clients in marginal or declining growth industries and geographic leads that were showing economic decline. To mask the fraudulent activity, transactions are entered as routine expenses, with the amounts varying in small, random increments. To further ensure anonymity, the funds are then laundered through a number of randomly selected clients who are offered discounted fees for processing the funds as simple cash transactions. Such services are needed by small businesses that need help implementing different types of financial or payroll software that are purchased, custom prepared and installed, with later training and a monthly maintenance and support package. After the pilot program business began to slow, but a suggestion from a disgruntled former employee of the fraudulent actions of the firm led investigators to monitor the transaction records of Local Blend and NewRealm that were completed between partners.

7. References

[1] Lakshminarayana Reddy Kothapalli Sondinti, Ravi Kumar Vankayalapati, Shakir Syed, Ramanakar Reddy Danda, Rama Chandra Rao Nampalli, Kiran Kumar Maguluri, & Yasmeen. (2024). Financial Optimization in the Automotive Industry: Leveraging Cloud-Driven Big Data and AI for Cost Reduction and Revenue Growth. The Bioscan, 19(Special Issue-1), 639–645. https://doi.org/10.63001/tbs.2024.v19.i02.S.I(1).pp639-645

[2] Burugulla, J. K. R. (2024). The Future of Digital Financial Security: Integrating AI, Cloud, and Big Data for Fraud Prevention and Real Time Transaction Monitoring in Payment Systems. MSW Management Journal, 34(2), 711-730.

[3] Annapareddy, V. N., & Sudha Rani, P. (2024). AI and ML Applications in RealTime Energy Monitoring and Optimization for Residential Solar Power Systems. Available at SSRN 5116062.

[4] Polineni, T. N. S., Ganti, V. K. A. T., Maguluri, K. K., & Rani, P. S. (2024). AI-Driven Analysis of Lifestyle Patterns for Early Detection of Metabolic Disorders. Journal of Computational Analysis and Applications, 33(8).

[5] Venkata Bhardwaj Komaragiri. (2024). Generative AI-Powered Service Operating Systems: A Comprehensive Study of Neural Network Applications for Intelligent Data Management and Service Optimization . Journal of Computational Analysis and Applications (JoCAAA), 33(08), 1841–1856. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/1861

[6] Vamsee Pamisetty. (2024). AI Powered Decision Support Systems in Government Financial Management: Transforming Policy Implementation and Fiscal Responsibility. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 1910–1925. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/1928

[7] Polineni, T. N. S. (2024). Integrating Quantum Computing and Big Data Analytics for Accelerated Drug Discovery: A New Paradigm in Healthcare Innovation. Journal of Artificial Intelligence and Big Data Disciplines, 1(1), 38-49.

[8] Paleti, S. Agentic AI in Financial Decision-Making: Enhancing Customer Risk Profiling, Predictive Loan Approvals, and Automated Treasury Management in Modern Banking.

[9] Challa, S. R. Behavioral Finance in Financial Advisory Services: Analyzing Investor DecisionMaking and Risk Management in Wealth Accumulation.

[10] Shyamala Anto Mary, P., Kalisetty, S., & Mandala, V. M. (2024). Advancing IoT Data Forecasting with Deep Learning Framework for Resilience Scalability and Real-World Applications. Srinivas and C, Chethana and B, Thevahi and Mandala, Vishwanadham and M, Balaji, Advancing IoT Data Forecasting with Deep Learning Framework for Resilience Scalability and Real-World Applications (November 15, 2024).

[11] Kannan, S., & Seenu, A. (2024). Advancing Sustainability Goals with AI Neural Networks: A Study on Machine Learning Integration for Resource Optimization and Environmental Impact Reduction. management, 32(2).

[12] Sambasiva Rao Suura (2024) Generative AI Frameworks for Precision Carrier Screening: Transforming Genetic Testing in Reproductive Health. Frontiers in Health Informa 4050-4069

[13] Nuka, S. T. (2024). Exploring AI and Generative AI in Healthcare Reimbursement Policies: Challenges, Ethical Considerations, and Future Innovations. International Journal of Medical Toxicology and Legal Medicine, 27(5), 574-584.

[14] Pallav Kumar Kaulwar. (2023). Tax Optimization and Compliance in Global Business Operations: Analyzing the Challenges and Opportunities of International Taxation Policies and Transfer Pricing. International Journal of Finance (IJFIN) - ABDC Journal Quality List, 36(6), 150-181. https://ijfin.com/index.php/ijfn/article/view/IJFIN_36_06_008

[15] Malempati, M., & Rani, P. S. Autonomous AI Ecosystems for Seamless Digital Transactions: Exploring Neural Network-Enhanced Predictive Payment Models.

[16] Sondinti, K., & Reddy, L. (2024). Financial Optimization in the Automotive Industry: Leveraging Cloud-Driven Big Data and AI for Cost Reduction and Revenue Growth. Financial Optimization in the Automotive Industry: Leveraging Cloud-Driven Big Data and AI for Cost Reduction and Revenue Growth (December 17, 2024).

[17] Challa, K. (2024). Neural Networks in Inclusive Financial Systems: Generative AI for Bridging the Gap Between Technology and Socioeconomic Equity. MSW Management Journal, 34(2), 749-763.

[18] Ramanakar Reddy Danda, Z. Y., Mandala, G., & Maguluri, K. K. Smart Medicine: The Role of Artificial Intelligence and Machine Learning in Next-Generation Healthcare Innovation.

[19] Karthik Chava, Kanthety Sundeep Saradhi. (2024). Emerging Applications of Generative AI and Deep Neural Networks in Modern Pharmaceutical Supply Chains: A Focus on Automated Insights and Decision-Making. South Eastern European Journal of Public Health, 20–45. https://doi.org/10.70135/seejph.vi.4441

[20] Sriram, H. K. (2023). Harnessing AI Neural Networks and Generative AI for Advanced Customer Engagement: Insights into Loyalty Programs, Marketing Automation, and Real-Time Analytics. Educational Administration: Theory and Practice, 29(4), 4361-4374.

[21] AI-Powered Revenue Management and Monetization: A Data Engineering Framework for Scalable Billing Systems in the Digital Economy . (2024). MSW Management Journal, 34(2), 776-787.

[22] Krishna AzithTejaGanti, V., Senthilkumar, K. P., Robinson L, T., Karunakaran, S., Pandugula, C., & Khatana, K. (2024). Energy-Efficient Real-Time Hybrid Deep Learning Framework for Adaptive Iot Intrusion Detection with Scalable and Dynamic Threat Mitigation. KP and Robinson L, Thomas and Karunakaran, S. and Pandugula, Chandrashekar and Khatana, Kavita, Energy-Efficient Real-Time Hybrid Deep Learning Framework for Adaptive Iot Intrusion Detection with Scalable and Dynamic Threat Mitigation (November 15, 2024).

[23] Chaitran Chakilam, Dr. P.R. Sudha Rani. (2024). Designing AI-Powered Neural Networks for Real-Time Insurance Benefit Analysis and Financial Assistance Optimization in Healthcare Services. South Eastern European Journal of Public Health, 974–993. https://doi.org/10.70135/seejph.vi.4603

[24] Nampalli, R. C. R., & Adusupalli, B. (2024). Using Machine Learning for Predictive Freight Demand and Route Optimization in Road and Rail Logistics. Library of Progress-Library Science, Information Technology & Computer, 44(3).

[25] Intelligent Supply Chain Optimization: AI Driven Data Synchronization and Decision Making for Modern Logistics. (2024). MSW Management Journal, 34(2), 804-817.

[26] Syed, S., Jayalakshmi, S., Kumar Vankayalapati, R., Mandala, G., Yadav, O. P., & Yadav, A. K. (2024). A Robust and Scalable Deep Learning Framework for Real-Time Iot Intrusion Detection with Adaptive Energy Efficiency and Adversarial Resilience. Available at SSRN 5077791.

[27] R. Daruvuri, K. Patibandla, and P. Mannem, "Leveraging unsupervised learning for workload balancing and resource utilization in cloud architectures," International Research Journal of Modernization in Engineering Technology and Science, vol. 6, no. 10, pp. 1776-1784, 2024.

[28] Avinash Pamisetty. (2022). Enhancing Cloudnative Applications WITH Ai AND Ml: A Multicloud Strategy FOR Secure AND Scalable Business Operations. Migration Letters, 19(6), 1268–1284. Retrieved from https://migrationletters.com/index.php/ml/article/view/11696

[28] Somepalli, S. (2021). Dynamic Pricing and its Impact on the Utility Industry: Adoption and Benefits. Zenodo. https://doi.org/10.5281/ZENODO.14933981

[29] Nampalli, R. C. R., & Adusupalli, B. (2024). AI-Driven Neural Networks for Real-Time Passenger Flow Optimization in High-Speed Rail Networks. Nanotechnology Perceptions, 334-348.

[30] Chaitran Chakilam, Dr. Aaluri Seenu, (2024) Transformative Applications of AI and ML in Personalized Treatment Pathways: Enhancing Rare Disease Support Through Advanced Neural Networks. Frontiers in Health Informa 4032-4049

[31] Maguluri, K. K., Pandugula, C., & Yasmeen, Z. (2024). Neural Network Approaches for Real-Time Detection of Cardiovascular Abnormalities.

[32] Koppolu, H. K. R. Deep Learning and Agentic AI for Automated Payment Fraud Detection: Enhancing Merchant Services Through Predictive Intelligence.

[33] Sriram, H. K. (2022). AI Neural Networks In Credit Risk Assessment: Redefining Consumer Credit Monitoring And Fraud Protection Through Generative AI Techniques. Migration Letters, 19(6), 1017-1032.

[34] P. Mannem, R. Daruvuri, and K. K. Patibandla, “Leveraging Supervised Learning in Cloud Architectures for Automated Repetitive Tasks.,” International Journal of Innovative Research in Science,Engineering and Technology, vol. 13, no. 10, pp. 18127–18136, Oct. 2024, doi: 10.15680/ijirset.2024.1311004.

[35] Chava, K. (2022). Redefining Pharmaceutical Distribution With AI-Infused Neural Networks: Generative AI Applications In Predictive Compliance And Operational Efficiency. Migration Letters, 19, 1905-1917.

[36] Yasmeen, Z., Machi, S., Maguluri, K. K., Mandala, G., & Reddy, R. (2024). Transforming Patient Outcomes: Cutting-Edge Applications of AI and ML in Predictive Healthcare. Transforming Patient Outcomes: Cutting-Edge Applications of AI and ML in Predictive Healthcare SEEJPH, 25, S1.

[37] Kishore Challa. (2024). Artificial Intelligence and Generative Neural Systems: Creating Smarter Customer Support Models for Digital Financial Services . Journal of Computational Analysis and Applications (JoCAAA), 33(08), 1828–1840. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/1860

[38] Danda, R. R., Nampalli, R. C. R., Sondinti, L. R. K., Vankayalapati, R. K., Syed, S., Maguluri, K. K., & Yasmeen, Z. (2024). Harnessing Big Data and AI in Cloud-Powered Financial Decision-Making for Automotive and Healthcare Industries: A Comparative Analysis of Risk Management and Profit Optimization.

[39] Malempati, M. (2022). Machine Learning and Generative Neural Networks in Adaptive Risk Management: Pioneering Secure Financial Frameworks. Kurdish Studies. Green Publication. https://doi. org/10.53555/ks. v10i2, 3718.

[40] Pallav Kumar Kaulwar. (2022). The Role of Digital Transformation in Financial Audit and Assurance: Leveraging AI and Blockchain for Enhanced Transparency and Accuracy. Mathematical Statistician and Engineering Applications, 71(4), 16679–16695. Retrieved from https://philstat.org/index.php/MSEA/article/view/2959

[41] Nuka, S. T. (2024). The Future of AI Enabled Medical Device Engineering: Integrating Predictive Analytics, Regulatory Automation, and Intelligent Manufacturing. MSW Management Journal, 34(2), 731-748.

[42] Sambasiva Rao Suura. (2024). Artificial Intelligence and Machine Learning in Genomic Medicine: Redefining the Future of Precision Diagnostics. South Eastern European Journal of Public Health, 955–973. https://doi.org/10.70135/seejph.vi.4602

[43] Kannan, S. The Convergence of AI, Machine Learning, and Neural Networks in Precision Agriculture: Generative AI as a Catalyst for Future Food Systems.

[44] Srinivas Kalisetty, D. A. S. Leveraging Artificial Intelligence and Machine Learning for Predictive Bid Analysis in Supply Chain Management: A Data-Driven Approach to Optimize Procurement Strategies.

[45] The Future of Banking and Lending: Assessing the Impact of Digital Banking on Consumer Financial Behavior and Economic Inclusion. (2024). MSW Management Journal, 34(2), 731-748.

[46] Paleti, S. Transforming Money Transfers and Financial Inclusion: The Impact of AI-Powered Risk Mitigation and Deep Learning-Based Fraud Prevention in Cross-Border Transactions.

[47] Polineni, T. N. S., Kumar, A. S., Maguluri, K. K., Koli, V., Valiki, D., & Ravikanth, S. (2024). A Scalable and Robust Framework for Advanced Semi Supervised Learning Supporting Universal Applications. Available at SSRN 5080654.

[48] Vamsee Pamisetty. (2023). Optimizing Public Service Delivery through AI and ML Driven Predictive Analytics: A Case Study on Taxation, Unclaimed Property, and Vendor Services. International Journal of Finance (IJFIN) - ABDC Journal Quality List, 36(6), 124-149. https://ijfin.com/index.php/ijfn/article/view/IJFIN_36_06_007

[49] Komaragiri, V. B. (2024). Data-Driven Approaches to Battery Health Monitoring in Electric Vehicles Using Machine Learning. International Journal of Scientific Research and Management (IJSRM), 12(01), 1018-1037.

[50] Maguluri, K. K., Ganti, V. K. A. T., & Subhash, T. N. (2024). Advancing Patient Privacy in the Era of Artificial Intelligence: A Deep Learning Approach to Ensuring Compliance with HIPAA and Addressing Ethical Challenges in Healthcare Data Security. International Journal of Medical Toxicology & Legal Medicine, 27(5).

[51] Annapareddy, V. N. (2022). Innovative Aidriven Strategies For Seamless Integration Of Electric Vehicle Charging With Residential Solar Systems. Migration Letters, 19(6), 1221-1236.

[52] Vankayalapati, R. K., Yasmeen, Z., Bansal, A., Dileep, V., & Abhireddy, N. (2024, December). Advanced Fault Detection in Semiconductor Manufacturing Processes Using Improved AdaBoost RT Model. In 2024 9th International Conference on Communication and Electronics Systems (ICCES) (pp. 467-472). IEEE.

[53] Reddy, J. K. (2024). Leveraging Generative AI for Hyper Personalized Rewards and Benefits Programs: Analyzing Consumer Behavior in Financial Loyalty Systems. J. Electrical Systems, 20(11s), 3647-3657.

[54] K. Patibandla, R. Daruvuri, and P. Mannem, "Streamlining workload management in AI-driven cloud architectures: A comparative algorithmic approach," International Research Journal of Engineering and Technology, vol. 11, no. 11, pp. 113-121, 2024.

[55] Satyaveda Somepalli. (2024). Leveraging Technology and Customer Data to Conserve Resources in the Utility Industry: A Focus on Water and Gas Services. Journal of Scientific and Engineering Research. https://doi.org/10.5281/ZENODO.13884891

[56] Burugulla, J. K. R. (2022). The Role of Cloud Computing in Revolutionizing Business Banking Services: A Case Study on American Express's Digital Financial Ecosystem. Kurdish Studies. Green Publication. https://doi. org/10.53555/ks. v10i2, 3720.

[57] Annapareddy, V. N., & Sudha Rani, P. (2024). AI and ML Applications in RealTime Energy Monitoring and Optimization for Residential Solar Power Systems. Available at SSRN 5116062.

[58] Venkata Krishna Azith Teja Ganti ,Kiran Kumar Maguluri ,Dr. P.R. Sudha Rani (2024). Neural Network Applications in Understanding Neurodegenerative Disease Progression. Frontiers in HealthInformatics, 13 (8) 471-485

[59] Komaragiri, V. B., Edward, A., & Surabhi, S. N. R. D. Enhancing Ethernet Log Interpretation And Visualization.

[60] Pamisetty, V. (2023). Intelligent Financial Governance: The Role of AI and Machine Learning in Enhancing Fiscal Impact Analysis and Budget Forecasting for Government Entities. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i10s(2).3480

[61] Ganti, V. K. A. T., Edward, A., Subhash, T. N., & Polineni, N. A. (2023). AI-Enhanced Chatbots for Real-Time Symptom Analysis and Triage in Telehealth Services.

[62] Daruvuri, R., Ravikumar, R., Mannem, P., & Aeniga, S. R. (2024). Augmenting Business Intelligence How AI and Data Engineering Elevate Power BI Analytics. International Journal of Innovative Research in Computer and Communication Engineering, 12(12), pp. 13012-13022.

[63] Challa, S. R. (2023). The Role of Artificial Intelligence in Wealth Advisory: Enhancing Personalized Investment Strategies Through DataDriven Decision Making. International Journal of Finance (IJFIN), 36(6), 26-46.

[64] Kalisetty, S., Pandugula, C., Sondinti, L. R. K., Mallesham, G., & Rani, P. S. (2024). AI-Driven Fraud Detection Systems: Enhancing Security in Card-Based Transactions Using Real-Time Analytics. Journal of Electrical Systems, 20, 1452-1464.

[65] Kannan, S. (2022). The Role Of AI And Machine Learning In Financial Services: A Neural Networkbased Framework For Predictive Analytics And Customercentric Innovations. Migration Letters, 19(6), 985-1000.

[66] Nuka, S. T. (2023). Generative AI for Procedural Efficiency in Interventional Radiology and Vascular Access: Automating Diagnostics and Enhancing Treatment Planning. Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi. org/10.53555/jrtdd. v6i10s (2), 3449.

[67] Malempati, M. (2022). AI Neural Network Architectures For Personalized Payment Systems: Exploring Machine Learning's Role In Real-Time Consumer Insights. Migration Letters, 19(S8), 1934-1948.

[68] Satyasree, K. P. N. V., & Kothpalli Sondinti, L. R. (2024). Mitigating Financial Fraud and Cybercrime in Financial Services with Security Protocols and Risk Management Strategies. Computer Fraud and Security, 2024(11).

[69] Challa, K. (2023). Transforming Travel Benefits through Generative AI: A Machine Learning Perspective on Enhancing Personalized Consumer Experiences. Educational Administration: Theory and Practice. Green Publication. https://doi. org/10.53555/kuey. v29i4, 9241.

[70] Somepalli, S. (2023). Power Up: Lessons Learned from World's Utility Landscape. Zenodo. https://doi.org/10.5281/ZENODO.14933958

[71] Chava, K., & Rani, D. P. S. (2023). Generative Neural Models in Healthcare Sampling: Leveraging AI-ML Synergies for Precision-Driven Solutions in Logistics and Fulfillment. Frontiers in Health Informa (6933-6952).

[72] Sriram, H. K., & Seenu, A. (2023). Generative AI-Driven Automation in Integrated Payment Solutions: Transforming Financial Transactions with Neural Network-Enabled Insights. International Journal of Finance (IJFIN), 36(6), 70-95.

[73] Shukla, A., Dubey, S., Nithya, P., Shankar, B., Vankayalapati, R. K., & Khatana, K. (2024). Edge-Optimized and Explainable Deep Learning Framework for Real-Time Intrusion Detection in Industrial Iot. Available at SSRN 5077557.