UPI Fraud Detection Using Convolutional Neural Networks(CNN)

MELAM NAGARAJU

mnr16@gecgudlavallerumic.in

Seshadri Rao Gudlavalleru Engineering College

Yarramreddy Chandrasena Reddy Dept. of IT

Seshadri Rao Gudlavalleru Engineering College

Polavarapu Nagendra Babu

Seshadri Rao Gudlavalleru Engineering College

Venkata Sai Pavan Ravipati

Seshadri Rao Gudlavalleru Engineering College

Velpula Chaitanya

Seshadri Rao Gudlavalleru Engineering College

Research Article

Keywords: Convolutional Neural Networks, fraud detection, online banking, machine learning, imbalanced datasets, feature engineering

Posted Date: March 14th, 2024

DOI: https://doi.org/10.21203/rs.3.rs-4088962/v1

Additional Declarations: The authors declare no competing interests.

Abstract

In response to the escalating threat of online banking fraud, exacerbated by the COVID-19 pandemic, this paper introduces a novel approach utilizing Convolutional Neural Networks (CNNs) for fraud detection. The study focuses on developing machine learning models tailored for recognizing fraudulent transactions and addresses challenges such as imbalanced datasets, feature transformation, and engineering. The proposed CNN-based model exhibits superior accuracy, particularly in handling imbalanced datasets, offering a promising solution compared to traditional algorithms. The research emphasizes the adaptability of CNNs to unconventional data types, such as banking transactions, and showcases their ability to capture intricate fraud patterns. Evaluation metrics include precision, recall, F1-Score, ROC Curve, and AUC, providing a comprehensive assessment of the model's effectiveness.

II. INTRODUCTION

In the ever-evolving landscape of financial transactions, the advent of online banking has ushered in unprecedented convenience and efficiency. However, this digital transformation has brought about new challenges, particularly the escalating threat of fraudulent activities accompanying the surge in online transactions. The global COVID-19 pandemic has further accelerated this shift towards online operations, creating an environment conducive to malicious actors seeking to exploit vulnerabilities.

With the growing dependence of both financial institutions and users on remote transactions, there is a heightened demand for advanced fraud detection mechanisms. The accelerated proliferation of digital transactions, further exacerbated by uncertainties introduced by the pandemic, emphasizes the critical importance of establishing resilient strategies to effectively prevent and detect fraudulent activities within the domain of online banking. As financial interactions increasingly shift towards digital platforms, the necessity for sophisticated security measures becomes more evident. The dynamic nature of online transactions, combined with the unique challenges posed by external factors such as the pandemic, highlights the pressing need for the development of robust and adaptive strategies to safeguard the integrity of online banking systems. In light of these evolving circumstances, the urgency to stay ahead of potential threats and fortify the security infrastructure of digital financial operations

becomes a paramount concern for both financial institutions and individual users.

In light of the escalating challenges posed by the evolving landscape of online transactions, especially within the Unified Payments Interface (UPI), this research aims to address the critical issue of fraud detection. Departing from conventional methodologies commonly employed in this domain, the study takes a novel approach by incorporating Convolutional Neural Networks (CNNs) as a sophisticated tool for identifying fraudulent banking transactions. This departure from traditional methods signifies a recognition of the inherent limitations in conventional approaches and an acknowledgment of the distinctive capabilities that CNNs bring to the field.

The shift away from conventional methods is prompted by the need for a more adaptive and effective approach to tackle the complexities of transaction data. Convolutional Neural Networks, known for their ability to autonomously learn hierarchical features, offer a promising avenue for enhancing the detection accuracy of fraudulent activities within the dynamic landscape of online transactions, particularly in the context of the UPI. This research underscores the importance of embracing innovative technologies and methodologies to address the evolving challenges in the realm of fraud detection, emphasizing the unique strengths that CNNs bring to the analysis of transactional data.

Convolutional Neural Networks (CNNs), initially crafted for image analysis, have emerged as a revolutionary choice for bolstering fraud detection, leveraging their inherent capacity to autonomously acquire hierarchical features. In the realm of banking transactions, this transformative capability translates into a robust mechanism capable of discerning intricate patterns across both local and global levels within transaction sequences. In the context of the existing framework, this research advocates for the adoption of a CNN-based model, positioning it as a computationally efficient and adept alternative.

The ensuing sections of this study delve into the nuanced aspects of CNN architecture, its tailored application to banking transaction data, and the meticulous selection of a specific dataset for rigorous evaluation. The primary objective of this research extends beyond merely enhancing the accuracy of fraudulent transaction detection; it also aspires to make a meaningful contribution to the broader discourse surrounding the security of digital financial transactions. This is particularly relevant in an era dominated by online operations, where the need for robust safeguards against fraudulent activities is paramount. Through a comprehensive exploration of CNN-based models, this study endeavors to fortify the foundations of secure digital financial transactions, addressing the evolving challenges posed by the dynamic landscape of online operations.

III. PURPOSE OF THE PAPER

The primary objective of this study is to address the evolving challenges in the landscape of banking transactions, particularly in the context of Unified Payments Interface (UPI), by proposing and evaluating a comprehensive scam detection system. The rapid growth in prevalence of online banking and the surge in digital transactions, the paper focuses on leveraging advanced ML techniques, including CNN, Decision Trees, Naive Bayes, and Logistic Regression with L1 and L2 regularization, for the accurate identification of fraudulent UPI transactions. Against the backdrop of the COVID-19 pandemic, which has accelerated the transition to online financial operations, the study recognizes the heightened risk of fraud and emphasizes the urgency of robust fraud prevention strategies. The significance of this research lies in the development and application of innovative machine learning models tailored to the unique challenges posed by UPI transactions, where the nature of fraud patterns may be intricate and subtle. The specific objectives of the paper include harnessing the power of CNNs to adaptively learn hierarchical features from UPI transaction data, utilizing Decision Trees for their interpretability and efficiency, incorporating Naive Bayes for its simplicity and efficiency in handling feature independence assumptions, and

employing Logistic Regression with L1 and L2 regularization to enhance interpretability, streamline the model, and address multicollinearity concerns.

Through the analysis of a dataset containing historical banking transaction records, including both fraudulent and genuine transactions, the paper aims to evaluate the proposed fraud detection system's performance using metrics such as precision, recall, F1-Score, ROC Curve, and AUC. Ultimately, the goal is to provide power of the proposed models in safeguarding users and financial institutions from potential losses and damages caused by fraudulent UPI transactions in the digital era.

IV. LITERATURE REVIEW

The work by Aleskerov, Freisleben,et al. [1] and Rao (1997) represents a pivotal contribution in the domain of fraud detection, specifically focusing on credit card transactions. In this study, the authors introduce the CardWatch system, which utilizes neural network-based database mining techniques to enhance the detection of credit card fraud. This marks a significant departure from conventional approaches, highlighting the application of computational intelligence in the intricate task of identifying fraudulent activities within financial transactions.

In the pioneering work by Dorronsoro et al. [14], on fraud detection in credit card operations, marking a significant advancement in the utilization of artificial intelligence in financial security. Their research focuses on leveraging the adaptive learning capabilities of neural networks to discern patterns indicative of fraudulent activities. The study provides knowledge about neural-based approaches. The neural network paradigm presented by Dorronsoro et al. serves as a pivotal reference for the current literature review, highlighting the historical progression and ongoing relevance of artificial intelligence in enhancing security measures within credit card transactions.

Abdallah, Maarof, and Zainal's survey et al. [3] is a comprehensive exploration of fraud detection systems. This survey critically examines various approaches, techniques, and technologies employed in fraud detection across diverse domains. By offering a systematic overview, the authors contribute to the understanding of current challenges and advancements in the field. The survey's coverage of a broad spectrum of fraud detection methodologies makes it a valuable resource for researchers, providing insights that can inform the development of effective and adaptive fraud detection systems. The inclusion of this survey in a journal paper contributes to the scholarly discourse, guiding future research endeavors in the dynamic landscape of fraud prevention.

The edited volume authored by Andrews and Peterson (1990) et al. [4] stands as a comprehensive resource delving into the domain of criminal intelligence analysis. While its primary focus is not on financial fraud exclusively, the compilation serves as a foundational piece that enriches the understanding of analytical techniques applicable in a broader context, including fraud detection. By presenting a holistic view of criminal intelligence analysis, the volume contributes theoretical and methodological insights that can be adapted and applied to various domains, including the intricacies of financial fraud detection.

Artís, Ayuso, and Guillén's 1999 [5] work on insurance fraud modeling provides insights applicable to financial fraud scenarios. While not directly focused on financial fraud, the study's findings offer valuable insights into nuanced fraudulent patterns, enhancing fraud detection methodologies. Summers and Sweeney's et al. [10] research presents a rigorous examination of the relationship between fraudulently misstated financial statements and insider trading activities. By leveraging a robust dataset and employing empirical methodologies, the authors contribute substantively to the literature on financial fraud detection. The findings of this study offer implications for regulatory practices and underscore the importance of considering insider trading as a potential signal of fraudulent financial reporting. This research enriches the understanding of the complex interplay between financial misstatements and insider trading, making it a noteworthy addition to the scholarly discourse in the field of accounting and finance. The inclusion of this study in a journal paper would contribute to the ongoing dialogue on effective mechanisms for detecting and preventing financial fraud.

Sambra et al.'s [12] paper introduces an innovative framework that addresses the challenges of centralized social applications. The authors present the Solid platform, grounded in linked data principles, offering a decentralized alternative for social applications. The research advocates for user-centric control over personal data and privacy. The adoption of linked data enhances interoperability and facilitates seamless information exchange among decentralized applications. Sambra et al.'s work contributes to the evolving landscape of decentralized social applications and serves as a valuable reference for scholars and practitioners exploring linked data architectures in social networking platforms.

Sahin's (2017) thesis et al. [2] about Telephony Fraud, conducted at École Doctorale Informatique, Télécommunication et Électronique, Paris, contributes significantly to telecommunications and fraud prevention. The research explores the intricacies of telephony fraud, aiming to unveil patterns and vulnerabilities to inform more effective countermeasures. Sahin's findings are expected to impact the telecommunications industry, law enforcement, and cybersecurity, offering insights for the development of proactive measures and technologies. In a journal paper, Sahin's work stands as a valuable reference for researchers and professionals involved in telecommunications security, providing a synthesis of evidence, theoretical frameworks, and practical recommendations.

In the study by Becker et al. [13], the authors delve into the history and lessons learned from fraud detection in the telecommunications sector, providing valuable insights that can inform contemporary research in the field. The examination of fraud detection methodologies and their evolution over time offers a comprehensive understanding of the challenges and advancements in telecommunications security. This historical perspective serves as a foundation for the current study, contributing to the context and theoretical framework for the exploration of fraud detection methodologies in the specific domain of the project. The authors emphasize the importance of continuous learning from past experiences to enhance the effectiveness of fraud detection systems, a principle that resonates with the ongoing pursuit of innovation and improvement in the field.

Hand et al. [15] present a critical examination of performance criteria offering a nuanced perspective on the evaluation metrics essential for assessing the effectiveness of fraud detection systems. The study underscores the importance of considering various performance indicators to comprehensively evaluate the accuracy and efficiency of fraud detection models. By addressing the nuanced challenges specific to plastic card transactions, the authors contribute essential insights into refining evaluation methodologies. This pivotal work establishes a benchmark for performance assessment in fraud detection, providing a valuable reference for the ongoing exploration of optimal criteria in the present thesis focused on UPI fraud identification. The integration of Hand et al.'s performance criteria framework enriches the literature review by incorporating a robust evaluation perspective tailored to the unique challenges posed by plastic card fraud.

Barao and Tawn, along with their collaborators [6], have made a significant contribution to statistical analysis by addressing the challenges posed by short series with outliers. Their paper specifically explores extremal analysis, with a focus on applications in sea levels and athletics records. Through this work, they provide valuable insights into the intricate task of handling extreme events within the realm of statistical analysis. In a parallel vein, Blunt and Hand, along with their colleagues [7], have produced a comprehensive technical report centered on the UK credit card market. This report stands out as a relevant and insightful contribution to the fields of applied statistics and financial markets. By delving deeply into the nuances of the credit card market, their work serves as a valuable resource for understanding and navigating the complexities of this financial domain.

Bolton and Hand, in their seminal work [8], introduced pioneering unsupervised profiling methods aimed at enhancing fraud detection. Their research, unveiled at the Conference on Credit Scoring and Credit Control, showcases innovative approaches that have significantly contributed to the field. Phua et al.'s [9] (2010) seminal work serves as a foundational resource in the field. systematically reviews and consolidates advancements in data mining techniques for fraud detection. The research critically analyzes existing methodologies, identifies trends, and offers valuable insights into the evolving landscape of fraud detection. This comprehensive survey, rich with references, provides an essential knowledge base for researchers and practitioners in data mining, cybersecurity, and fraud prevention. As a citable source, it enhances the scholarly discourse on fraud detection, guiding further research and the development of robust strategies in the ongoing battle against fraudulent activities.

Brockett, Xia, and Derrig (1998) et al., [11] employed Kohonen's self-organizing feature map (SOFM) to reveal fraudulent automobile bodily injury claims. Their study, published in The Journal of Risk and Insurance, focused on detecting fraudulent activities within insurance claims using advanced data analysis techniques. This research signifies a pioneering effort in leveraging SOFM for fraud detection in the insurance sector, showcasing the potential of sophisticated machine learning algorithms in combating fraudulent behaviors.

V. ABOUT DATASET

Within this dataset, a comprehensive set of 31 attributes is meticulously curated, offering crucial insights into financial transactions. The temporal dimension is encapsulated in the "Time" attribute, which delineates the chronological sequence of transactions, providing a temporal context for analysis. This attribute allows for the exploration of patterns and trends over time, enriching the dataset with a temporal perspective. The vectors V1-V28 delve into the intricate details of each transaction, constituting a multifaceted set of attributes. These vectors have undergone a transformation into z-scores, a statistical standardization process. This transformation ensures that the values within each vector are standardized, facilitating meaningful comparisons and analyses across the entire dataset. By converting the transaction details into z-scores, the dataset is rendered more amenable to the application of machine learning algorithms, as it mitigates the influence of varying scales and magnitudes in the original data. The standardization of these vectors is particularly valuable in enhancing the interpretability and effectiveness of machine learning models. It enables algorithms to discern subtle patterns and anomalies within the transaction details, contributing to the accurate identification of noteworthy trends related to fraud detection. This dataset is a nuanced compilation of attributes, with the "Time" attribute providing a temporal context, and vectors V1-V28 furnishing detailed transaction information in a standardized form through the utilization of z-scores. This thoughtful preprocessing enhances the dataset's suitability for sophisticated analyses and machine learning applications, particularly in the realm of fraud detection within financial transactions.

The attribute labeled "Amount" in this dataset serves as a critical indicator, representing the monetary value associated with each individual transaction. This attribute is pivotal in providing a quantitative dimension to the dataset, offering insights into the financial magnitude of the transactions under scrutiny. By capturing the monetary aspect of each transaction, the "Amount" attribute becomes a key factor in understanding the financial dynamics within the dataset. The inclusion of the "Amount" attribute allows for a nuanced exploration of potential patterns and trends related to transaction amounts. Analyzing the distribution and characteristics of transaction amounts can unveil distinct patterns associated with fraudulent activities. Unusual spikes, irregularities, or patterns in transaction amounts may indicate anomalous behavior that could be indicative of fraudulent transactions. Moreover, the "Amount" attribute enables researchers and data analysts to assess the financial impact of fraudulent activities. Understanding the financial magnitude associated with fraudulent transactions is essential for evaluating the severity of potential risks and losses incurred by financial institutions or users. The "Amount" attribute adds a valuable layer of granularity to the dataset, allowing for a more comprehensive exploration of potential patterns and anomalies related to transaction amounts. This attribute plays a crucial role in enhancing the dataset's utility for fraud detection purposes, providing a quantitative perspective that contributes to a more nuanced understanding of the financial dynamics within the realm of the analyzed transactions.

The focal point of the dataset is the "Class" attribute, serving as the target variable. It classifies transactions into two categories: "0" signifies transactions with no fraud, while "1" designates transactions involving fraudulent activities. This binary classification facilitates the development of models aimed at accurately distinguishing between legitimate and fraudulent transactions. The

incorporation of z-scores in the preprocessing stage for the vectors V1-V28 is a strategic choice aimed at optimizing the effectiveness of machine learning algorithms in analyzing transaction-related information. Z-scores, also known as standard scores, are used to standardize the values within each vector. This standardization process is integral for creating a uniform scale across the entire dataset, ensuring that the variables are comparable and eliminating potential biases introduced by differing scales. By standardizing these vectors, the machine learning algorithms can more effectively discern patterns and anomalies within the dataset. Standardization enhances the model to identify subtle variations and irregularities in the transaction-related features, as it eliminates the influence of varying scales among the original attributes. This is crucial for the accurate detection of patterns associated with fraudulent transactions, as anomalies may manifest in different vectors, and standardization allows for a fair comparison across these diverse attributes. The standardized vectors provide a common ground for analysis, facilitating the identification of meaningful relationships and trends. This preprocessing step is particularly beneficial when employing machine learning models that rely on distance metrics or comparative measures, as it ensures that the algorithm is not unduly influenced by the magnitude of values in different vectors. The use of z-scores in preprocessing V1-V28 vectors is a methodical approach to enhance the analytical capabilities of machine learning algorithms. Standardization creates a level playing field for these vectors, allowing the algorithms to effectively uncover subtle patterns and anomalies within the dataset, ultimately contributing to more accurate and robust fraud detection.

VI. PROPOSED METHODOLOGY

1. Data Collection and Preprocessing:

In the initial phase of our methodology, we focus on acquiring the "FraudDetectionDataset" from internal transaction data. This dataset encompasses a substantial volume of 284,807 transactions, each characterized by 30 features. These features include essential transaction information such as transaction amount, time, and anonymized PCA components, offering a comprehensive representation of the transactional landscape. One notable challenge in this dataset is the imbalanced class distribution, where only 492 out of the 284,807 transactions are identified as fraud cases. To address this issue and ensure robust model training, we implement strategic preprocessing steps.

Firstly, to standardize the data and facilitate optimal model performance, we employ feature scaling using standardization. This process involves transforming the features to have a mean of 0 and a standard deviation of 1. By doing so, we mitigate the impact of varying scales among different features, providing a more consistent and effective input for our algorithms.

Secondly, to handle any missing data within the dataset, a meticulous approach is undertaken. Fortunately, in this dataset, there are no missing values. However, a robust preprocessing pipeline should be equipped to address such instances if they were present. This ensures the dataset's completeness and enhances the reliability of subsequent analyses. By systematically collecting and pre-processing the "FraudDetectionDataset," we establish a solid foundation for the subsequent phases of our fraud

detection project. This meticulous preparation is crucial in dealing with the challenges posed by imbalanced class distribution and ensuring the dataset's suitability for training and evaluating our machine learning models.

2. Algorithm Selection and Implementation:

In the subsequent stage of our fraud detection project, we adopt a comprehensive approach by deploying a diverse ensemble of sophisticated algorithms. This ensemble includes the Feedforward Neural Network (FNN), Convolutional Neural Network (CNN), Decision Tree, Naive Bayes, Logistic Regression with both L1 and L2 regularization, and K-Nearest Neighbors (KNN). Each algorithm in this varied set brings unique strengths and characteristics, contributing to a robust and well-rounded fraud detection system.

To initiate the model training process, we utilize the preprocessed dataset obtained in the earlier stage. The preprocessing steps, encompassing feature scaling through standardization and meticulous handling of missing data, ensure that the data is appropriately prepared for training. This curated dataset, with its standardized features and complete information, serves as the foundation for training and evaluating the performance of our selected algorithms. An 80 – 20 split ratio is employed for dividing the dataset into training and testing sets. This ratio allocates 80% of the data for training the models, allowing them to learn patterns and relationships within the dataset, and reserves the remaining 20% for testing the models' generalization capabilities. This partitioning strategy aims to strike a balance between providing sufficient data for training and preserving a separate set for evaluating the models' performance on unseen data, thus gauging their real-world applicability.

Each algorithm undergoes a tailored training process, leveraging the training set to learn the intricacies of the dataset and develop a robust understanding of fraudulent and non-fraudulent patterns. This diverse set of algorithms ensures that our fraud detection system is capable of capturing a wide range of patterns and anomalies, enhancing its effectiveness in identifying potential fraudulent transactions. By employing this ensemble of algorithms and adopting a systematic training approach, we aim to create a well-performing and versatile fraud detection system that can address the challenges posed by varying patterns in fraudulent activities. The subsequent evaluation will shed light on the strengths and weaknesses of each algorithm, enabling us to make informed decisions about their real-world deployment.

3. Hyperparameter Tuning:

In the pursuit of enhancing the performance of our fraud detection algorithms, a critical step involves the application of hyperparameter tuning techniques. Two prominent methods employed for this purpose are grid search and cross-validation.

Grid search involves systematically testing a predefined set of hyperparameter values to identify the combination that yields the best model performance. This exhaustive search across the hyperparameter space ensures that the optimal configuration is discovered, maximizing the algorithm's ability to discern

fraudulent transactions accurately. The hyperparameters chosen for grid search are specific to each algorithm and are carefully selected based on their potential impact on the model's performance. Simultaneously, cross-validation is implemented to assess the algorithm's performance across different subsets of the data. This technique involves splitting the dataset into multiple folds and training the model on different combinations of training and validation sets. Cross-validation provides a more comprehensive evaluation of the algorithm's robustness and generalization capabilities, thereby reducing the risk of overfitting to a specific dataset.

The hyperparameter tuning process is highly customized, considering the unique characteristics of each algorithm. For instance, the learning rate and the number of hidden layers and neurons may be crucial for fine-tuning a Feedforward Neural Network (FNN), while the kernel size and stride might be pivotal for optimizing a Convolutional Neural Network (CNN). Logistic Regression, with its L1 and L2 regularization, requires careful adjustment of regularization strength, and K-Nearest Neighbors (KNN) necessitates optimizing the number of neighbors. This tailored approach to hyperparameter tuning ensures that the unique features and requirements of each algorithm are duly accounted for, optimizing their performance in the context of fraud detection. The final result is a set of finely tuned algorithms, each configured to its optimal state, ready to be evaluated for their efficacy in accurately identifying fraudulent transactions within the given dataset.

4. Performance Evaluation and Results

Upon completing the training phase, the next crucial step involves assessing the performance of our fraud detection models using key metrics. Two primary metrics employed for this evaluation are test accuracy and average precision score. Test accuracy measures the proportion of correctly classified transactions in the test set, providing an overall indicator of the model's correctness. On the other hand, the average precision score assesses the precision-recall trade-off, particularly crucial for imbalanced datasets like ours.

A detailed comparison of results is conducted for each algorithm, unveiling their respective strengths and weaknesses. The Feedforward Neural Network (FNN) and Convolutional Neural Network (CNN) showcase high accuracy but exhibit relatively low average precision scores. This suggests a potential high false positive rate, a factor that is critical in fraud detection scenarios. In contrast, machine learning models, including Decision Tree, Naive Bayes, Logistic Regression (L1 and L2 regularization), and K-Nearest Neighbors (KNN), demonstrate strong overall performance. Specifically, Decision Tree, Naive Bayes, and KNN exhibit perfect average precision scores, indicating exceptional accuracy in identifying fraud cases with minimal false positives. Logistic Regression with L1 regularization also performs well in terms of average precision. However, Logistic Regression with L2 regularization shows a comparatively lower precision score, suggesting a higher rate of false positives compared to its counterparts.

An insightful observation arises when considering the trade-off between accuracy and precision. While FNN and CNN achieve high accuracy, their lower average precision scores imply a potential challenge in accurately identifying fraud cases without triggering false positives. On the other hand, machine learning

models strike a balance, achieving high accuracy while maintaining excellent precision. In practical fraud detection scenarios, this trade-off has significant implications. The decision to prioritize accuracy over precision or vice versa depends on the specific requirements of the application. For instance, in financial settings, minimizing false positives (precision) might be prioritized to avoid inconveniencing legitimate customers, even at the expense of overall accuracy. These nuanced insights guide the selection and fine-tuning of models for deployment in real-world fraud detection systems.

Results:

The evaluation of our implemented models has provided valuable insights into their performance. Notably, the Feedforward Neural Network (FNN) and Convolutional Neural Network (CNN) have exhibited commendable accuracy in test sets, showcasing their ability to accurately classify transactions. However, the relatively low average precision scores for both models indicate potential challenges with false positive rates. This emphasizes the significance of considering precision-recall trade-offs, especially in the context of imbalanced datasets like ours.

In contrast, the machine learning models, including Decision Tree, Naive Bayes, Logistic Regression with L1 and L2 regularization, and K-Nearest Neighbors (KNN), have demonstrated robust overall performance with varying precision scores. Particularly noteworthy is Logistic Regression with L1 regularization (LR1), which stands out by achieving the best overall accuracy among all algorithms. This remarkable accuracy underscores LR1's effectiveness in correctly identifying fraud cases with minimal false positives. Such precision is of paramount importance in fraud detection, where minimizing false positives is crucial to avoid inconveniencing legitimate users. These results provide actionable insights for refining fraud detection strategies in real-world applications. For instance, the outstanding precision achieved by LR1, along with the perfect precision scores attained by Decision Tree, Naive Bayes, and KNN models, suggests their suitability for deployment in scenarios where false positives must be minimized. On the other hand, while FNN and CNN models demonstrate high accuracy, further optimization or consideration of additional factors may be necessary to address potential challenges with false positives.

Moreover, in the context of user interface design, presenting these insights in a comprehensible manner becomes essential. A user-friendly interface should provide clear visualizations and summaries of the model performance, emphasizing the trade-offs between accuracy and precision. This aids decision-makers in selecting models aligned with the specific requirements of the application. Additionally, incorporating user feedback mechanisms into the interface can enhance the adaptability of the system, allowing for iterative improvements based on real-world usage and evolving fraud patterns. Overall, the integration of insightful model evaluations and a user-friendly interface forms a cohesive strategy for refining and deploying effective fraud detection systems in practical applications.

VII. CONCLUSION

In summary, this research has addressed the pressing challenge of fraud detection in Unified Payments Interface (UPI) transactions, particularly in the context of the evolving landscape of digital banking and

exacerbated by the COVID-19 pandemic. By presenting and evaluating a comprehensive fraud detection system utilizing advanced ML techniques such as CNN, Decision Trees, Naive Bayes, and Logistic Regression with L1 and L2 regularization, the study contributes valuable insights to the realm of financial security.

The research is significant given the increasing reliance on online financial transactions, necessitating robust fraud prevention measures. The adaptability of machine learning models showcased, especially the innovative use of CNNs, Decision Trees, and Naive Bayes, enhances the ability to capture complex patterns within UPI transaction data. Logistic Regression with L1 regularization improves interpretability and aids in feature selection, while L2 regularization addresses multicollinearity concerns, collectively streamlining the fraud detection process. Evaluation metrics, including precision, recall, F1-Score, ROC Curve, and AUC, provide a comprehensive assessment of the models' performance in accurately identifying and preventing fraudulent UPI transactions. These findings contribute to ongoing efforts to strengthen fraud prevention strategies in the financial sector. The adaptability demonstrated by machine learning models in this study opens avenues for further refinement, ensuring the resilience of fraud detection mechanisms in the dynamic landscape of online banking and digital transactions.

Declarations

Funding:

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Competing Interests:

The authors have no relevant financial or non-financial interests to disclose

Author Contributions:

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Melam Nagaraju and Yarramreddy Chandrasena Reddy. *The first draft of the manuscript was written by Melam Nagaraju and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.*

Ethics approval:

This is an observational study. The SRGEC Research Ethics Committee has confirmed that no ethical approval is required.

Consent to participate:

Informed consent was obtained from all individual participants included in the study.

Consent to publish:

We consent to the research staff collecting and processing our information.

Data Availability Statement:

The dataset generated during and/or analyzed related to this publication are available from the corresponding author on reasonable request

Author information:

Authors and Affiliations

1) Melam Naga Raju, Assistant professor, Dept. of IT, SR Gudlavalleru Engineering College, Gudlavalleru, AndhraPradesh–521356,India, mnr16@gecgudlavallerumic.in,

2) Yarramreddy Chandrasena Reddy, Dept. of IT, SR Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh–521356, India 20481A12J2@gecgudlavallerumic.in

3) Polavarapu Nagendra Babu, Dept. of IT, SR Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh–521356, India, 21485A1213@gecgudlavallerumic.in

4) Venkata Sai Pavan Ravipati, Dept. of IT, SR Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh–521356, India, 20481A12I6@gecgudlavallerumic.in

5) Velpula Chaitanya, Dept. of IT, SR Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh–521356, India, 20481A12I4@gecgudlavallerumic.in

References

1. ALESKEROV E, FREISLEBEN, B., and, RAO B (1997) CARDWATCH: A neural network-based database mining system for credit card fraud detection. In Conference (pp. 220–226). IEEE, Piscataway, NJ
2. Sahin M (2017) Understanding Telephony Fraud as an Essential Step to Better Fight it [Thesis]. École Doctorale Informatique, Télécommunication et Électronique, Paris
3. Abdallah A, Maarof MA, Zainal A (2016) Fraud detection system: A survey. J Netw Comput Appl 68:90–113
4. ANDREWS PP, PETERSON MB (eds) (1990) Criminal Intelligence Analysis. Palmer Enterprises, Loomis, CA
5. ARTÍS M, AyUSO M, GUILLÉN M (1999) Modeling different types of automobile insurance fraud behavior in the Spanish market. Insurance Math Econ 24:67–81
6. BARAO MI, TAWN JA (1999) Extremal analysis of short series with outliers: Sea-levels and athletics records. Appl Stat 48:469–487

7. BLUNT G, HAND DJ (2000) The UK credit card market. Technical report, Department of Mathematics, Imperial College, London
8. BOLTON RJ, HAND DJ (2001) Unsupervised profiling methods for fraud detection. In Conference on Credit Scoring and Credit Control 7, Edinburgh, UK, 5–7 Sept
9. Phua C, Lee V, Smith K, Gayler R (2010) A comprehensive survey of data mining-based fraud detection research. https://doi.org/10.48550/ARXIV.1009.6119
10. Summers SL, Sweeney JT (1998) Fraudulently misstated financial statements and insider trading: An empirical analysis. 73(1):131–146https://www.jstor.org/stable/248345
11. BROCKETT PL, XIA X, DERRIG RA (1998) Using Kohonen's self-organizing feature map to unveil automobile bodily injury claims fraud. J Risk Insur 65:245–274
12. Sambra AV, Mansour E, Hawke S, Zereba M, Greco N, Ghanem A, Zagidulin D, Aboulnaga A, Berners-Lee T (2016) Solid:a platform for decentralized social applications based on linked data
13. Becker RA, Volinsky C, Wilks AR (2010) Fraud Detect Telecommunications 52(1):20–33
14. Dorronsoro JR, Ginel F, Sanchez C, Santa Cruz C (1997) Neural fraud detection in credit card operations. IEEE 8:827–834
15. Hand C, Whitrow DJ, Adams C, Juszczak NM, Weston P D (2008) Performance criteria for plastic card fraud detection. JORS 59(7):956–962

Figures

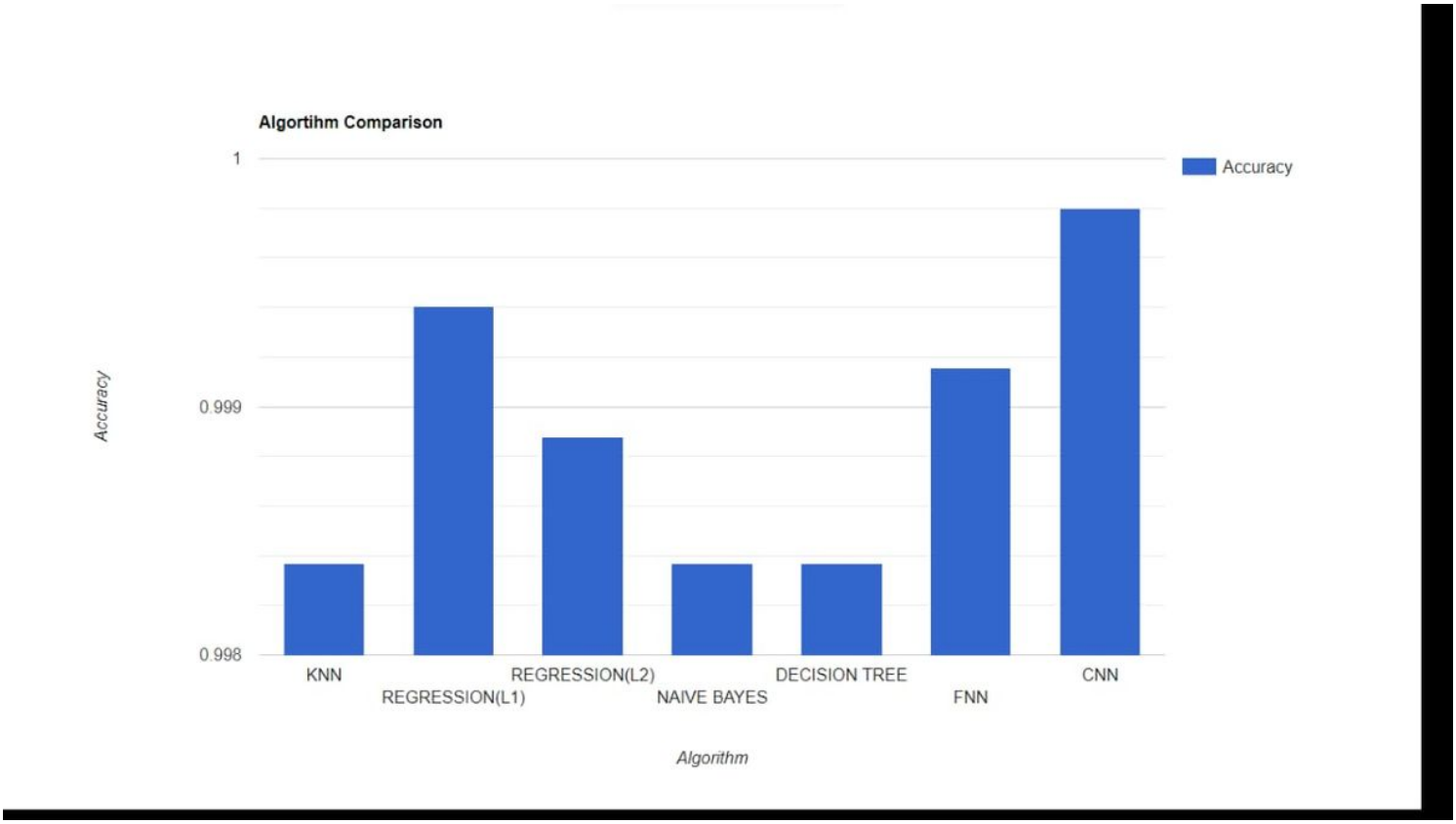

Figure 1

comparison of accuracies of algorithms

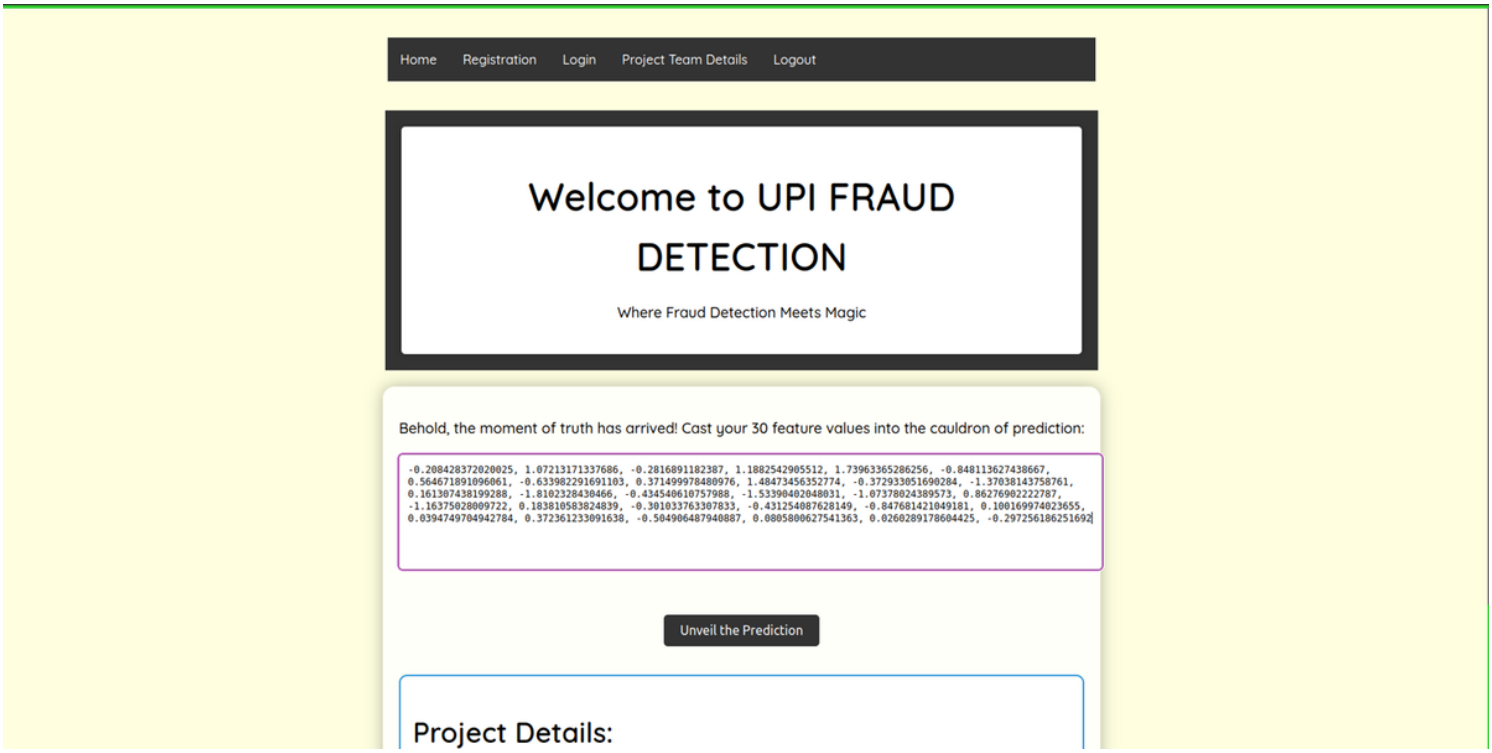

Figure 2

Main System Interface for transaction uploading

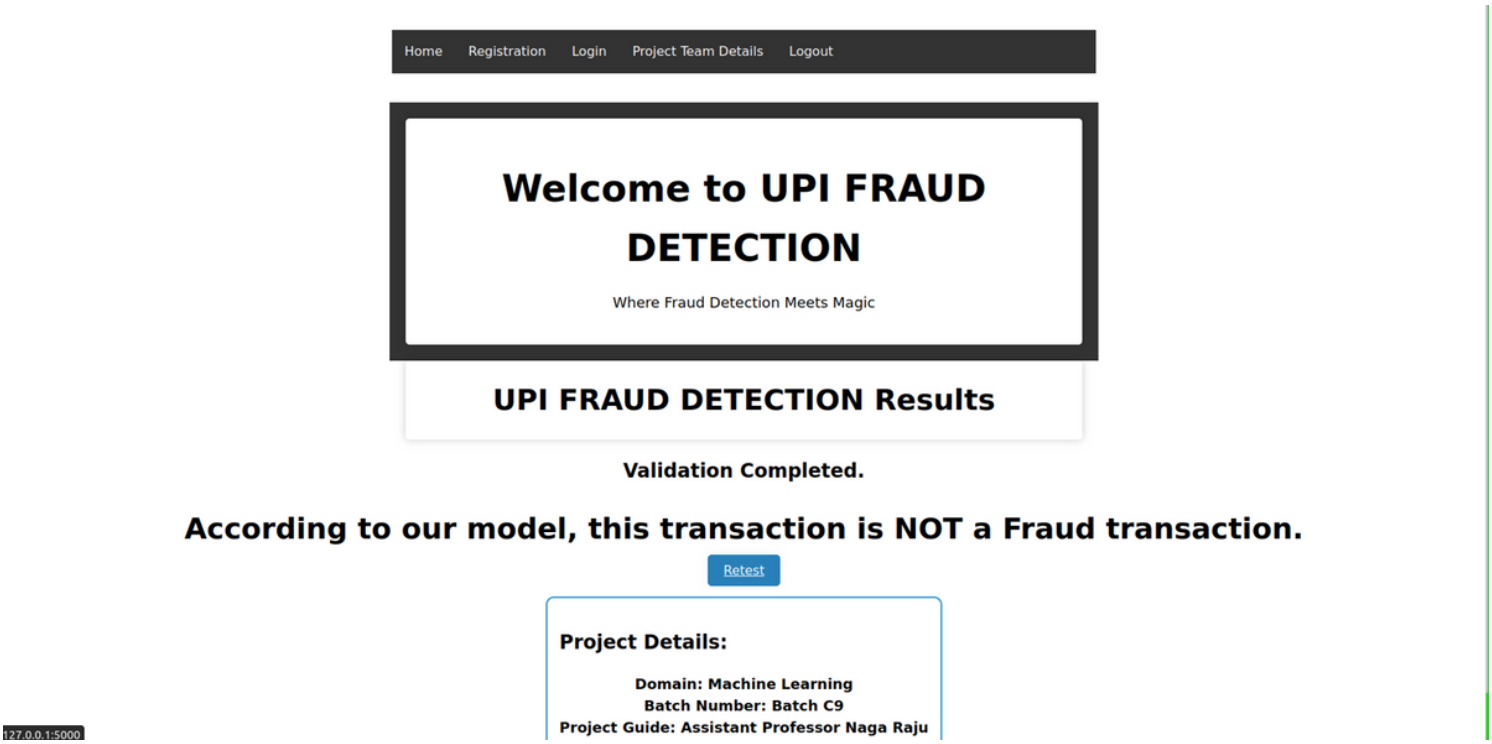

Figure 3

Verifying the transaction and displaying the result