Predictive Analytics for Digital Transactions

Sasikala C., Anil Kumar Bandi, Ambica Cheluru, Aswartha Reddy Settipi,
Durga Bhavani Vanka and Tarun Kumar Reddy Peram
Department of Computer Science and Engineering, Srinivasa Ramanujan Institute of Technology (SRIT), Anantapur, Andhra Pradesh, India

Keywords: Choice Trees, Irregular Woodlands, Angle Assistance, Protection Safeguarding Models, Models of Straightforwardness Include Deep Neural Networks (DNN), Recurrent Neural Networks (RNN), Federated Learning (FL), Financial Fraud Detection, Explainable Artificial Intelligence (XAI), AI Algorithms.

Abstract: In the domain of monetary misrepresentation location, accomplishing harmony among straightforwardness and security is basic. Conventional methodologies frequently neglect to give both elevated degrees of exactness and clear, justifiable clarifications for navigation, all while safeguarding delicate information. They attempt to uncover the solutions that United Learning (FL) and Reasonable Computer-based Intelligence (XAI) provide on these particular challenges. Financial institutions utilizing quantitative predictions must deeply trust their models, and XAI provides models for them. However, Unified Learning considers the construction of AI models to a collection of dispersed data sources where sensitive financial data is properly siloed. In detail, this study looks at how different algorithms, which include Deep Neural Networks (DNN), Recurrent Neural Networks (RNN), Decision Trees, Random Forests, and Support Vector Machines, are utilized in fraud detection tasks and how these algorithms are integrated into the multi-task learning framework. In addition, the study investigates fusion methods for models such as Stochastic Gradient Descent (SGD) and its variants. This study investigates how financial institutions could enhance fraud detection systems while ensuring transparency, confidentiality, and compliance with data protection laws by integrating the best of both XAI and FL worlds.

1 INTRODUCTION

This article examines the combination of Explainable AI (XAI) and Federated Learning (FL) with the goal of increasing fraud detection capabilities within financial institutions while enhancing transparency, regulatory compliance, and data security. AI-enabled fraud detection provides high accuracy, however, as explained previously, there is a significant lack of explain ability, which complicates matters within the extremely controlled financial sector. To foster trust and compliance with regulations like GDPR, XAI ensures that decision-making by AI systems is more explainable and transparent. On the other hand, FL enables the development of AI models on data held in silos, thereby preserving privacy and minimizing the risk of security breaches. Established financial institutions can now build effective systems for accurate fraud detection without compromising security, explain ability, or precision by integrating XAI and FL. The models selected for the study include decision trees, recurrent neural networks (RNN), deep neural networks (DNN), and gradient boosting models with a focus on the FL framework for AI. The focus is also on optimization methods such as stochastic gradient descent (SGD) to make them more efficient. Lastly, the paper proposes a framework for responsible use of AI in financial fraud detection by achieving a balance of data privacy, transparency, and overall system performance.

2 THE ROLE OF THIS WEB APPLICATION

The primary purpose of this study is to assess the effectiveness of a novel combined approach using Federated Learning (FL) and Explainable AI (XAI) in payment fraud detection systems. There are existing techniques for fraud detection and prevention that work, but they tend to be centralized

C., S., Bandi, A. K., Cheluru, A., Settipi, A. R., Vanka, D. B. and Peram, T. K. R.
Predictive Analytics for Digital Transactions.
DOI: 10.5220/0013922500004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 5*, pages 56-61
ISBN: 978-989-758-777-1

and obfuscated, which can lead to challenges with privacy and compliance laws. FL does allow for data processing to be conducted in a more decentralized manner, but XAI claims to provide trustable AI conclusions. The focus of this research is on the comparison of different AI models, including Deep Learning Neural Networks (DNNs), Recurrent Neural Networks (RNNs), Decision Trees, Random Forest, and Gradient Boosting, which will all be executed under FL framework. In order to improve the performance of the models, additional parameters such as Stochastic Gradient Descent (SGD) will also be utilized. It is the objective of this work to also illustrate an E2E framework for AI augmented payment fraud detection featuring accuracy, transparency, data privacy, and regulatory compliance.

3 LITERATURE REVIEW

As scientists strive to enhance model simplicity, security, and predictive accuracy, the combination of Federated Learning (FL) and Explainable Artificial Intelligence (XAI) has recently gained considerable attention, especially in the realm of financial fraud detection. Traditional AI methods have primarily depended on centralized models for identifying misrepresentation, where sensitive financial data is stored and managed on centralized servers. However, these methods face challenges related to regulatory compliance and security, particularly with stringent data protection laws like the GDPR. A promising solution to these challenges is Federated Learning, which facilitates the collaborative development of models without sharing raw data among participants. FL enables various financial institutions or organizations to collaboratively build AI models using their local datasets while keeping their most sensitive information private, thus addressing security concerns while leveraging extensive data resources. Since the variety of value-based designs employed by various organizations is essential in spotting unusual activities, this widely recognized learning paradigm is especially useful in detecting financial extortion. Simultaneously, the test lies in guaranteeing that such models are interpretable and straightforward, as monetary (Balcıoğlu, Y. S) foundations should give clarifications to their mechanized choices, particularly when these choices can have critical legitimate and monetary outcomes. The requirement for interpretability in misrepresentation location models has prompted a developing interest in XAI. Conventional AI calculations, especially profound learning models, are frequently seen as "secret elements" because their (Bodker A et al., 2022) dynamic cycles are not effectively justifiable by people. This absence of straightforwardness creates difficulties in managed areas like money, where it isn't simply vital to make exact expectations but additionally to give clear defenses to those forecasts. (Demertzis et al., 2022 XAI expects to resolve this issue by creating procedures and models that permit leaders to comprehend and believe the expectations made by simulated intelligence frameworks. Different procedures have been proposed to upgrade the interpretability of mind- boggling models, for example, highlight significance examination, nearby clarification techniques like LIME (Neighborhood Interpretable (Guo et al., 2024) Model rationalist Clarifications), and SHAP (SHapley Added substance Clarifications). These techniques offer a method for making sense of individual expectations, making it clearer why a specific exchange was hailed as fake or not. By giving partners straightforward bits of knowledge into the dynamic cycle, XAI not only upgrades trust in computerized misrepresentation identification frameworks (Hasan et al., 2024) yet in addition helps meet administrative prerequisites in regard to responsibility and decency in a computer-based intelligence-driven direction. As far as algorithmic commitments to misrepresentation location, an extensive variety of AI models have been investigated. Profound Brain Organizations (DNNs) have been widely utilized because of their capacity to catch complex examples and learn progressive portrayals of information. These models (Koetsier et al., 2022) have shown great outcomes in distinguishing misrepresentation, especially in conditions where the false way of behaving is unobtrusive or advances over the long run. Nonetheless, (Kollu et al., 2023) DNNs additionally face difficulties connected with interpretability, as they can be exceptionally perplexing and hard to make sense of.

Repetitive Brain Organizations (RNNs), especially Lengthy Transient Memory (LSTM) organizations, have additionally been utilized in misrepresentation (Lakhan etal., 2023) recognition undertakings that include consecutive information, like exchange chronicles. RNNs are successful in demonstrating fleeting conditions, which is basic in monetary extortion location, as deceitful exercises frequently unfurl after some time and show consecutive examples.

While RNNs offer benefits as far as transient examination, they likewise experience the ill effects

of interpretability issues, prompting a developing interest in coordinating XAI procedures with RNN-based models to offer more straightforward misrepresentation discovery arrangements. Other conventional AI procedures, for example, Choice Trees, (Mothukuri et al., 2021) Arbitrary Woods, and Angle Supporting techniques, have additionally been generally utilized in misrepresentation locations. Choice Trees are well known because of their intrinsic interpretability; their treelike design considers simple perceptions of choice ways. Be that as it may, their exhibition can corrupt while taking care of enormous, high-layered datasets, prompting the utilization of group techniques like Irregular Timberlands and Inclination (Raval et al., 2023) Helping Machines (GBM). These techniques, while further developing precision, present intricacy, making them harder to decipher. In any case, there have been propels in posthoc interpretability techniques for troupe models, for example, highlighting significance scores and proxy models, which have helped address the compromise between model exactness and logic. In addition, the utilization of group models has been displayed to further develop recognition (Sai et al., 2023) rates by joining the qualities of different models and lessening the gamble of overfitting.

4 IMPLEMENTATIONS

4.1 Flow Chart

A flowchart is a visual representation of the processes occurring within a system or project. It illustrates the various steps involved. The flowchart starts and concludes at the terminal points, which are depicted using oval shapes. Decision-making steps are represented by diamond shapes. Rectangular boxes indicate the processes that occur on the website. Processes that are adjacent to each other are sequential. Figure 1 Shows the Flow chart of application.

4.2 Database Connectivity

To store and access data from the server we require a database connection and we implanted below code snippet below provide the connection. This code creates a new mysqli object, specifying the database server, username, password, and database name. The connection is then verified, and an error message is displayed if the connection fails.

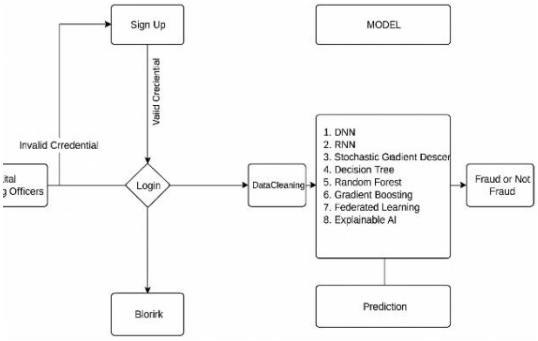

Figure 1: Flow Chart of Application.

4.3 Fetching Data

To fetch data from the database we implemented the following code snippet to get the data and load it in the frontend pages. This query retrieves the user's data from the users table, based on their unique user_id. The resulting data is then processed and displayed within the application. The shows Figure 2 Register page.

Figure 2: Register Page.

4.4 Front end

The frontend of our web application was built using HTML, CSS, JavaScript, and jQuery. HTML provided the structural foundation, while CSS was used for styling and layout. JavaScript and jQuery were utilized for dynamic client-side functionality, enhancing user interaction and experience. Our frontend design aimed to provide an intuitive and user- friendly interface, allowing users to seamlessly navigate and utilize the application's features. The Figure 3 shows Login Page.

Figure 3: Login Page.

4.5 User Credentials Validation

This is an example code snippet of JavaScript used in our application for front-end. This code snippet verifies credentials and logs in the students and faculty by sending a request to the database. It verifies the user credentials with in the browser before sending to the server for backend verification. The shows Figure 4 Home page.

Figure 4: Home Page.

5 RESULTS

The interfaces of this progressive web application are shown below Figure 5 and 6.

Figure 5: Model Training.

After selecting a certain algorithm, we calculate their accuracies based on the result of the result of the accuracies we choose which algorithm is best for fraud detection. The process of choosing the appropriate algorithm for fraud detection is illustrated in Figure 6, while the final output of the system is demonstrated on the prediction page shown in Figure 7.

Figure 6: Model Selection.

Figure 7: Prediction Page.

The below analytics shows Figure 8 and 9 the performance of the web application. In case the given values are legitimate then it shows the No fraud transaction.

Figure 8: Result 1.

In case the given values aren't legitimate then it shows the fraud transaction.

Figure 9: Result 2.

6 CONCLUSIONS

By ensuring data privacy through decentralized model training without exposing individual data, federated learning (FL) is enhanced by explainable AI (XAI), which makes AI-driven decisions more interpretable. This collaboration guarantees the development of reliable, interpretable, and legally compliant fraud detection systems. The study illustrates that while deep learning models like deep neural networks (DNNs) and recurrent neural networks (RNNs) offer high precision, they often lack transparency. In contrast, traditional models such as decision trees and random forests provide explain ability but may fall short in precision. By integrating these models into a federated learning framework, a hybrid approach can achieve a balance of explain ability, precision, and data protection. These advancements offer financial institutions a roadmap for implementing effective and regulatory-compliant fraud detection technologies, adhering to standards like the CCPA and GDPR.

7 ACKNOWLEDGMENT

We extend our heartfelt thanks to Dr. C. Sasikala, an assistant professor of computer science and engineering at Srinivasa Ramanujan Institute of Technology, for his invaluable guidance and support in making this research a success.

REFERENCES

Ahmed, A. A., & Alabi, O. O. (2024). Secure and Scalable Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review. IEEE Access, 12, 102219–102241.https://doi.org/10.1109/ACCESS.2024.3429205

Ali, S., Li, Q., & Yousafzai, A. (2024). Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey. Ad Hoc Networks, 152, 103320. https://doi.org/10.1016/J.ADHOC.2023.103320

Attanayaka, D. (2022). A novel anomaly detection mechanism for Open radio access networks with Peer-to- Peer Federated Learning. Laturi.Oulu.Fi. https://oulurepo.oulu.fi/handle/10024/21293

Balcıoğlu, Y. S. (1 C.E.). Revolutionizing Risk Management AI and ML Innovations in Financial Stability and Fraud Detection. Https://Services.IgiGlobal.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/979-8-3693-4382- Ch006,109–138. https://doi.org/10.4018/979-8-3693-4382-1.CH006

Bodker, A., Connolly, P., Sing, O., Hutchins, B., Townsley, M., & Drew, J. (2022). Card-not-present fraud: using crime scripts to inform crime prevention initiatives. Security Journal, 36(4), 1. https://doi.org/10.1057/S41284-022-00359-W

Demertzis, K., Iliadis, L., Kikiras, P., & Pimenidis, E. (2022). An explainable semi-personalized federated learning model. Integrated Computer-Aided Engineering, 29(4), 335–350. https://doi.org/10.3233/ICA-220683

Guo, W., & Jiang, P. (2024). Weakly Supervised anomaly detection with privacy preservation under a Bi- Level Federated learning framework. Expert Systems with Applications, 254, 124450. https://doi.org/10.1016/J.ESWA.2024.124450

Hasan, M., Rahman, M. S., Janicke, H., & Sarker, I. H. (2024). Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis. Blockchain: Research and Applications, 5(3), 100207. https://doi.org/10.1016/J.BCRA.2024.100207

Koetsier, C., Fiosina, J., Gremmel, J. N., Müller, J. P., Woisetschläger, D. M., & Sester, M. (2022). Detection of anomalous vehicle trajectories using federated learning. ISPRS Open Journal of Photogrammetry and Remote Sensing, 4, 100013. https://doi.org/10.1016/J.OPHOTO.2022.100013

Kollu, V. N., Janarthanan, V., Karupusamy, M., & Ramachandran, M. (2023). Cloud-Based Smart Contract Analysis in FinTech Using IoT-Integrated Federated Learning in Intrusion Detection. Data 2023, Vol. 8, Page 83, 8(5), 83. https://doi.org/10.3390/DATA8050083

Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., Alkhayyat, A., & Wang, W. (2023). Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare. IEEE Journal of Biomedical and Health Informatics, 27(2), 664–672. https://doi.org/10.1109/JBHI.2022.3165945

Marry, P., Mounika, Y., Nanditha, S., Shiva, R., & Saikishore, R. (2024). Federated Learning-Driven Decentralized Intelligence for Explainable Anomaly Detection in Industrial Operations. 2nd International Conference on Sustainable Computing and Smart

Systems, ICSCSS 2024 - Proceedings, 874–880. https://doi.org/10.1109/ICSCSS60660.2024.10625289

Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619640. https://doi.org/10.1016/J.FUTURE.2020.10.007

Raval, J., Bhattacharya, P., Jadav, N. K., Tanwar, S., Sharma, G., Bokoro, P. N., Elmorsy, M., Tolba, A., & Raboaca, M. S. (2023). RaKShA: A Trusted Explainable LSTM Model to Classify Fraud Patterns on Credit Card Transactions. Mathematics 2023, Vol. 11, Page 1901, 11(8),1901. https://doi.org/10.3390/MATH11081901

Sai, C. V., Das, D., Elmitwally, N., Elezaj, O., & Islam, M. B. (2023) Explainable Ai-Driven Financial Transaction Fraud Detection Using Machine Learning and Deep Neural Networks. https://doi.org/10.2139/SSRN.4439980