Temporal Convolutional Networks for Detecting Patterns of Fraudulent Activities in Time-Series Transaction Data

1st Smitha Kannur Ashok
Data Analytics, Industrial and Systems Engineering
The State University of New York at Buffalo
Buffalo, United States
smithaka@buffalo.edu

***Abstract*— *The identification of fraudulent activity has become a critical issue in an increasingly digitalized world, particularly in financial, e-commerce, and other transaction-based systems. Using sophisticated machine learning models is vital because traditional fraud detection techniques frequently fail to identify intricate patterns that change over time. The objective of the present research is to identify changing fraudulent patterns in time-series transaction data by using Temporal Convolutional Networks (TCNs). TCNs are a promising tool in the field of fraud detection because they are excellent at modelling temporal dependencies. This study examines the foundations of TCNs, their flexibility in responding to evolving fraudulent activities, and offers comparisons with more established approaches as well as real-world case studies. The study also looks at interpretability, providing some insight into how TCNs might transform fraud detection and improve security in systems that rely on transactions.*

Keywords*— *intricate patterns, fraudulent activity, transaction-based systems, traditional fraud detection techniques, time Series transaction data, temporal convolutional networks (TCNs), temporal dependencies, security,

I. Introduction

Beyond cybersecurity, there are many reasons to look into the use of Temporal Convolutional Networks (TCNs) for patterns of fraudulent activity detection in time-series transaction data. Fraud has far-reaching consequences that affect financial stability, consumer trust, and data privacy in our fast digitalizing world. As such, investigating novel methods of fraud detection is not only necessary but also urgent.

This research is valuable because it has the potential to completely change how we protect transaction-based systems, which are essential to both the daily operations of individuals and modern economies. Our ability to model and adjust to temporal dependencies with TCNs will help us tackle a fundamental problem: the dynamic nature of fraud. This invention could lower financial losses, safeguard private information, and increase confidence in online transactions. Furthermore, it provides insights into how fraud detection can be advanced with emerging technologies, with applications ranging from e-commerce to healthcare and beyond.

This investigation's wider implications go beyond specific businesses and sectors. It supports the continuous worldwide endeavour to strengthen digital ecosystems against con artists who constantly modify their methods. In the end, using TCNs for fraud detection is a way to strengthen the trust that supports our digitalized world and goes beyond simple technological advancement.

II. Critical Knowledge Gaps in Current Fraud Detection Techniques

The efficacy of fraud prevention and mitigation is impacted by the multiple knowledge gaps in the techniques currently used to address fraud detection. A number of significant gaps in knowledge prevent the problem from being fully resolved:

A. Temporal Understanding

The temporal dimensions of fraudulent activities are frequently poorly understood by current fraud detection techniques. Due to their inability to fully capture the dynamic and time-sensitive nature of fraud, they frequently miss fraudulent transactions and produce false positives. Techniques that can efficiently simulate temporal dependencies and adjust to evolving fraudulent patterns are required.

B. Complex Pattern Recognition

The ability of many current techniques to identify complex, non-linear patterns in transaction data is constrained. The strategies used by scammers are always changing, so it's difficult for conventional methods to stay relevant. More advanced models that can spot hidden patterns even when they are deeply ingrained in the data are needed to close this gap.

C. Real-time Monitoring

A lot of the techniques currently in use are not capable of real-time monitoring. Fraudulent activity may go undetected for a longer period of time if they are restricted to batch processing or sporadic updates. Monitoring in real time is necessary to minimise the effects of fraud and act quickly.

D. Adaptability

Conventional fraud detection techniques may find it difficult to adjust to new kinds of fraud or evolving strategies. They frequently rely on established norms and patterns, which are insufficient to handle the constantly changing field of fraudulent activity. Systems that are more flexible and self-learning are required.

E. Techniques for Preserving Privacy

As data privacy gains importance, there aren't many approaches that can effectively detect fraud while protecting the privacy of sensitive data. Finding the right balance between accuracy and privacy is very difficult.

III. Related work

Vatsa, Vishal [1] et al. (2007) highlight the necessity of intrusion detection techniques while addressing the shortcomings of conventional security measures against attacks. It presents a framework that views the relationship between intrusion detection systems and intruders as a multi-phase game in which both parties seek to maximise their gains. The study, which focuses on credit card fraud detection, suggests a two-tiered architecture that combines game theory and rule-based techniques. This method views intruders as rational adversaries and uses game theory to predict their optimal behaviour for more effective fraud detection than classical game theory, which assumes static optimal strategies.

Mansoor Ahmed [2] et al. (2021) discusses the serious effects that digital fraud has on the financial sector as well as on consumers, especially about online banking. Financial institutions all over the globe are actively trying to improve their capacity for detecting and discouraging digital fraud considering the growing reliance on online financial transactions. Fraud deterrence concentrates on a system's capacity to resist fraudulent attempts, whereas fraud detection is essentially a reactive process that seeks to identify ongoing malicious activities. This work introduces an Intimation Rule-Based (IRB) alert generation algorithm that classifies alerts according to severity levels and focuses on the crucial element of fraud deterrence. This solution presents an ontology-based model for financial fraud detection and deterrence, utilizing a rich domain knowledge base and rule-based reasoning.

J. O. Awoyemi [3] et al. (2017) The critical issue of financial fraud—more especially, credit card fraud in online transactions—is discussed in this paper. It draws attention to the difficulties in detecting credit card fraud, which are caused by highly skewed data sets and behaviors that are always changing. Using a highly skewed dataset of credit card fraud, the study examines how well three classification methods—Naïve Bayes, k-Nearest Neighbor, and Logistic Regression—perform. An approach to hybrid sampling is used to deal with the skewness. The findings show that while Logistic Regression performs at 54.86% accuracy rate, Naïve Bayes and k-Nearest Neighbor achieve accuracy rates of 97.92% and 97.69%, respectively, outperforming Logistic Regression. This study provides information on efficient fraud detection techniques when dealing with extremely unbalanced credit card transaction data.

Ogwueleka, F. N. [4] (2011), highlights data mining, and more especially a neural network technique, is good at creating models or patterns from input data, the study uses it to tackle credit card fraud. The research creates a neural network architecture for a credit card fraud detection system using the self-organizing map neural network (SOMNN) technique, which is based on an unsupervised method. Using transaction data, this method generates four clusters: low, high, risky, and high-risk. In comparison to other statistical models and two-stage clusters, the credit card fraud detection watch, utilising SOMNN, detects over 95% of fraud cases with minimal false alarms, according to the receiver-operating curve (ROC) analysis. According to the study's findings, the credit card fraud detection watch performs comparably to other detection software while demonstrating higher levels of efficiency.

Diwakar Tripathi [5] et al. (2017) focuses on the importance of online web advertising as a significant source of income for internet applications and the increasing risk posed by phishing attempts, which try to trick users into visiting phoney websites to steal sensitive data. Using the PhishTank database within the web advertising network and the Apriori algorithm for association rule mining, the study presents a novel architecture for web fraud detection. The suggested architecture shows promising results in terms of accuracy, error rate, memory usage, and search time through extensive experiments using web access logs. The results point to the new approach's potential efficacy in identifying and reducing web fraud within online ad networks.

Yashvi Jain [6] et al. (2019) discusses the growing risk of fraud brought on by the increased use of plastic and digital money, especially credit cards, which has resulted in significant financial losses on a global scale. Fraudsters consistently come up with new techniques despite the many safeguards in place, which highlights the necessity of a reliable fraud detection system that responds promptly and accurately. In addition to outlining several detection methods, such as Support Vector Machine, Artificial Neural Networks, Bayesian Network, K-Nearest Neighbour, Hidden Markov Model, Fuzzy Logic Based System, and Decision Trees, the study presents the idea of credit card fraud. The study finds shortcomings in current models and suggests better ways to improve credit card fraud detection through a thorough review and comparative analysis based on quantitative metrics like accuracy, detection rate, and false alarm rate.

Bertrand Lebichot [7] et al. (2019) In spite of the relatively low incidence rate, the paper highlights the possibility of substantial financial losses when discussing the problem of credit card fraud. It emphasises the necessity of accurate and flexible Fraud Detection Systems (FDS) that can handle the variety of fraudster behaviour across various payment systems, nations, and demographic groups. In light of the high expense of creating data-driven FDSs, deep transfer learning techniques for credit card fraud detection are examined in this paper. It focuses specifically on moving classification models that have been trained on e-commerce transactions to face-to-face transactions. The study presents two domain adaptation methods in the context of a deep neural network framework and evaluates their efficacy in comparison to three cutting-edge benchmarks using a large dataset that spans five months and more than 80 million in-person and online transactions supplied by a major card issuer.

Zhang Xinwei [8] et al. (2021) In addressing the substantial financial impact of credit card transaction fraud, the paper highlights the necessity of sophisticated fraud detection systems. The primary contribution is the creation of a deep learning architecture-based fraud detection system that employs a novel feature engineering approach based on homogeneity-oriented

behaviour analysis (HOBA). Utilising an actual dataset from a significant Chinese commercial bank, the research performs a comparative evaluation of the efficacy of the suggested framework. According to experimental results, the methodology is not only practical and effective, but it can also detect a higher number of fraudulent transactions at a reasonable false positive rate than benchmark methods. Credit card issuers can effectively detect fraudulent transactions, protect customer interests, and reduce fraud losses by utilising this methodology.

Joy Iong-Zong Chen [9] et al. (2021) The article discusses the growing financial losses brought on by the global increase in financial fraud, especially considering the increasing use of online services. The study suggests a sophisticated financial fraud detection system built on deep learning algorithms and the Deep Convolution Neural Network (DCNN) scheme to address these issues. The goal is to increase the accuracy of detection, particularly when dealing with big data analytics, high-speed computing, and unknown attack patterns. An actual credit card fraud dataset is used to compare the suggested model with other machine learning and deep learning models that are currently in use. The experimental results demonstrate the effectiveness of the DCNN-based scheme in improving fraud detection in large volumes of data, with a remarkable 99% detection accuracy achieved in 45 seconds.

Hosein_Fanai [10] et al. (2023) The article discusses the rise in fraudulent transactions brought on by the expansion of online payment options and e-commerce, highlighting the necessity of automated fraud detection systems to reduce monetary losses. The study suggests a two-stage framework for fraud detection that combines supervised deep learning techniques with a deep Autoencoder as a representation learning method. Through input data embedding into a lower-dimensional representation, the framework seeks to improve fraud detection systems' accuracy and robustness. Experiments show that the suggested method outperforms baseline classifiers trained on the original data, improving the performance of deep learning-based classifiers. Interestingly, models built with the deep Autoencoder perform better than models built with datasets derived from principal component analysis (PCA) and existing models, demonstrating the usefulness of the deep Autoencoder in improving the performance of fraud detection systems.

Jian Chen [11] et al. (2018) Present-day credit card detection techniques typically rely on the concept of classification, necessitating a training dataset that is balanced and includes both positive and negative samples. Nonetheless, we frequently obtain extremely skewed datasets with minimal fraud. In this paper, we aim to address this situation by utilising deep learning techniques. After obtaining representations of typical transactions using sparse autoencoder (SAE), we use these representations to train a generative adversarial network (GAN). To determine whether a transaction is authentic or fraudulent, we ultimately apply the combination of the SAE and the GAN discriminator. The outcomes of the experiment demonstrate that our solution works better than the other cutting-edge one-class techniques.

IV. Proposed Methodology

One of the main obstacles in the quest for more efficient fraud detection is the requirement to handle temporal dependencies in transaction data. Conventional techniques frequently fail to capture the dynamic and time-sensitive nature of fraudulent activity. We suggest using Temporal Convolutional Networks (TCNs) as a strong substitute to close this knowledge gap and solve the fraud detection issue.

A. Effective Temporal Dependency Modelling

TCNs are well known for their ability to effectively model temporal dependencies. Recurrent neural networks (RNNs) use sequential processing, whereas TCNs use convolutional layers to simultaneously capture dependencies across multiple time steps. Because of their design, TCNs can understand complex temporal patterns, which makes them ideal for the dynamic world of fraud.

B. Adaptability to Changing Patterns

To avoid discovery, scammers constantly adjust and change their strategies. TCNs are built to be flexible and adjust over time. Their capacity to draw insights from past data while staying alert to fresh patterns fits in with the dynamic nature of fraud detection, allowing the system to effectively react to new threats.

C. Real-time Monitoring and Alerting

TCNs can be used to continuously analyze incoming transaction data to address the problem of real-time monitoring. This real-time capability helps to minimise the possible impact of fraud by quickly identifying and responding to fraudulent activities as they happen.

D. Interpretability and Explainability

TCNs are more than just potent black-box models. By using methods like saliency maps and feature attribution, they can make their decision-making process more transparent. This closes the interpretability gap in the data by assisting fraud analysts in comprehending and verifying the reasons behind a transaction's flagging as fraudulent.

V. Contributions

There is potential for major advancements in both application and methodology from the study of Temporal Convolutional Networks (TCNs) in fraud detection:

A. Application Contribution

1) Monitoring and alerting for fraud in real-time: The investigation seeks to facilitate quick fraud detection and response by integrating TCNs for real-time monitoring. This has immediate application value in that it lessens the impact of fraudulent activities on organisations as well as financial losses and reputational harm.

2) Improved Interpretability and Trust: A more transparent and reliable fraud detection system is developed when interpretability techniques are added in addition to TCNs. For fraud analysts and other stakeholders who depend on the system's judgements and justifications for validation, this is extremely valuable.

B. Methodological Contribution

1) TCNs for identifying Fraud: The use of TCNs in fraud detection adds to the expanding corpus of research on applying

cutting-edge neural network architectures to challenging real-world problems. This methodological breakthrough provides new insights into the practical applications of deep learning on temporal data.

2) Enhanced Precision in Fraud Detection: A significant increase in the accuracy of fraud detection is anticipated to be one of the investigation's main contributions. Because TCNs efficiently model temporal dependencies, they can more accurately detect evolving fraudulent patterns, which lowers the number of false positives and false negatives.

3) Using Explainable AI (XAI) to Identify Fraud: More transparent and comprehensible AI systems can be developed by combining XAI techniques with TCNs. Beyond fraud detection, the methodological contribution has wider implications for machine learning and artificial intelligence, fields where explainability is becoming more and more important.

VI. Broader Impacts

The following sectors and research areas could benefit from this work's successful investigation in addition to fraud detection:

The potential for cross-industry insights is one of its most important contributions. Diverse industries can benefit from the adaptation and application of fraud detection lessons learned and creative solutions, which will strengthen their resistance to new threats and difficulties.

Utilising TCNs for fraud detection advances the investigation of sophisticated neural network topologies for practical problem-solving. This methodological development may encourage further researchers to use deep learning in a variety of domains, such as speech recognition, image recognition, natural language processing, and more.

Furthermore, the investigation highlights the critical importance of robust data security with state-of-the-art fraud detection techniques. The ideas and practices developed to protect transaction data can be extended to other domains where data security and integrity are essential. This can help with the defence of the country, the protection of critical infrastructure, and the security of private government data.

Finally, resolving analogous issues in other domains can be greatly aided by the ethical and legal considerations in the context of fraud detection systems. Regarding data ethics, digital rights, and regulatory compliance, for example, it can be helpful to have insights on how to strike a balance between the necessity for security and privacy and ethical considerations.

References

[1] Vatsa, Vishal, Shamik Sural, and Arun K. Majumdar. "A rule-based and game-theoretic approach to online credit card fraud detection." *International Journal of Information Security and Privacy (IJISP)* 1.3 (2007): 26-46.

[2] Ahmed, Mansoor, et al. "A semantic rule based digital fraud detection." *PeerJ Computer Science* 7 (2021): e649.

[3] J. O. Awoyemi, A. O. Adetunmbi and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, 2017, pp. 1-9, doi: 10.1109/ICCNI.2017.8123782.

[4] Ogwueleka, Francisca Nonyelum. "Data mining application in credit card fraud detection system." *Journal of Engineering Science and Technology* 6.3 (2011): 311-322.

[5] Tripathi, Diwakar, Bhawana Nigam, and Damodar Reddy Edla. "A novel web fraud detection technique using association rule mining." *Procedia computer science* 115 (2017): 274-281.

[6] Jain, Yashvi, et al. "A comparative analysis of various credit card fraud detection techniques." *International Journal of Recent Technology and Engineering* 7.5 (2019): 402-407.

[7] Lebichot, Bertrand, et al. "Deep-learning domain adaptation techniques for credit cards fraud detection." *Recent Advances in Big Data and Deep Learning: Proceedings of the INNS Big Data and Deep Learning Conference INNSBDDL2019, held at Sestri Levante, Genova, Italy 16-18 April 2019*. Springer International Publishing, 2020.

[8] Zhang, Xinwei, et al. "HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture." *Information Sciences* 557 (2021): 302-316.

[9] Chen, Joy Iong-Zong, and Kong-Long Lai. "Deep convolution neural network model for credit-card fraud detection and alert." *Journal of Artificial Intelligence and Capsule Networks* 3.2 (2021): 101-112.

[10] Fanai, Hosein, and Hossein Abbasimehr. "A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection." *Expert Systems with Applications* 217 (2023): 119562.

[11] J. Chen, Y. Shen and R. Ali, "Credit Card Fraud Detection Using Sparse Autoencoder and Generative Adversarial Network," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2018, pp. 1054-1059, doi: 10.1109/IEMCON.2018.8614815.