A Comprehensive Review on Generative Models for Anomaly Detection in Financial Data

Ankur Mahida

Subject Matter Expert (SME), Barclays

Abstract: ***Anomaly detection in the financial industry is one of the most critical aspects of identifying fraudulent transactions, outliers, and other uncommon patterns that might suggest some illegal action. Traditional techniques need help catching complicated financial data abnormalities with high dimensionality, often delivering incorrect results. Introducing more advanced generative modeling techniques that can learn the unique underlying distribution of average financial data to analysis acts as a more reliable approach. Through mimicking usual data points, these models generate random values when parameterized with a given set of characteristics; thereby, these become anomalies whose probability of being caused by the learned distribution is extremely low. This review delivers a detailed and accurate description of the state - of - the - art innovative generative models used in financial anomaly detection, such as autoencoders, GANs, normalizing flows, energy - based models, and more. The strengths and weaknesses of the given approaches are appraised. The following paragraph discusses the challenges embedded in frameworks for creating and deploying generative models, including interpretability, the protection of privacy, working with multidimensional data, and scarcity of data. Generative models can enhance the accuracy of anomaly prediction. However, researchers must adapt the algorithms to anomaly forecasts in complex market data. Targeted measures to solve the imperfections of generative models will fully unravel the potential ideal contemporary detection system that ensures lower false positives and false negative rates. Many financial institutions already employ powerful machine learning models to address financial crimes, such as fraud, money laundering, and insider trading. Still, turning it from academic promise to practical use could reduce most of these significantly.***

Keywords: anomaly detection, generative models, financial data, autoencoders, GANs, normalizing flows

1. Introduction

Anomaly detection, which reveals any data instance's oddity, is the most crucial process for financial data analysis. This way, institutions may manage to carry out the checking activities, and they will be able to recognize frauds like money laundry and insider trading. Nevertheless, financial data can be regarded as complex and multidimensional, raising several challenges to anomaly detection. The approaches or techniques, such as the simple statistics outliers and the basic machine learning models, only consider a few nonlinear dependencies and patterns in the financial data. This results in high false alarms and sometimes misdiagnosis in a healthy individual. As an advanced technique, one would need generative modeling methods that will be able to learn the Underlying distribution of the financial information as standard data. Models like GANs, normalizing flows, autoencoders, and energy - based models are the generative kind that can mold the complexity of financial data to some extent. Generative models can build robust models of average data points, and any data point with a small probability of being generated from the distribution will, as a result, be detected as an anomaly. This review seeks to provide a detailed assessment of the latest high - end generative models in financial anomaly detection. This chapter covers the strengths and disadvantages of different productive mode - ling approaches. Currently, the most encountered problems in building and applying such models cover the matters of interpretability, data privacy, multidimensionality of data etc., and data scarcity. Although generative models have a noticeable potential for anomaly detection development, applying more complex approaches to particular money data is still necessary. This survey aims to exert a balanced view of the milestones achieved so far along with the gaps that might take note of the records to date; the goal of using generative models to be accomplished to detect anomalies in the financial sector accurately and at the right time without any preference will be made possible.

2. Problem Statement

The problem of anomaly search on financial data represents several difficulties because of the complexity inherent in financial transactions, which have multiple dimensions. Financial data combines continuous, categorical, and temporal features across dimensions like the number of transactions, the type of merchant, customer demography data, and timestamp [1]. The data depicts the intricate interconnectedness with its repeated cycles and patterns, which traditional methods cannot grasp. In extreme cases, constructing an exact joint distribution of the normality of stock financial data is challenging [2]. As fraudulent transactions are likely to be significantly outweighed by legitimate ones, there is also a drastic inequality in social class. Despite processing a large selection of normal and abnormal data types, attaining an efficient model is extremely difficult since only some examples can be gathered from the field. Outlier detection and simple neural networks cannot be used to keep track of more sophisticated features introduced by real - time financial data [3]. These two tools do not capture the distributional movements and cannot distinguish between normal fluctuations. Such occurs to the detriment of the decision - making effectiveness of the technique in practice. Data augmentation is a valuable strategy that uses additional sources to enhance the limited data.

Nevertheless, we need more advanced generative models to accommodate complex data across multiple dimensions and related datasets to achieve an efficient approach. By accurately representing the joint distribution, generative models can communicate synonymous low - occurring (anomaly) probability data with a very low likelihood of being pulled from that distribution [4]. On the other hand, this model will only approximate the actual distribution of real - world financial data precisely and efficiently, which is still a significant challenge from the research point of view. Developing generative approaches in addition to this type of accurate anomaly detection is made possible, which takes into account the great multidimensionality of financial datasets.

3. Solution

Generative models present an exception detection technique where the models learn the distribution of average financial data. Therefore, the generative models can decide the probability of a new data instance being generated from the given distribution through this distribution [5]. Points that point to unusual things are most likely marked as anomalies as their probability is very low.

The Autoencoders reduce data to a latent space and recover it again. Encode and decode neural networks are trained on average data. That's why abnormalities in the test time cause significant reconstruction errors resulting from the deviation of the standard data distribution [6].

With the GANs, a generator network synthesizes fake data that matches or surpasses the actual data. The job of the discriminator network is to detect if it's real or not affected. When used for anomaly detection, GANs are taught to learn only from data that does not have anomalies. The discriminator determines what is fake, unlike the actual coded data and the normal one [7].

Normalizing flows turn data into a standard distribution through invertibility operations. Estimation of density provides a probability distribution function that is used in the detection of anomalies [8].

In energy - based models, anomaly detection is done through the energy function, where average points have lower energy, and the anomalies are high - energy outliers [9].

The main strength of generative methods is their ability to capture the unconstrained, multidimensional distribution of the standard data [10]. This brings in the added advantage of more refined anomaly detection tuned to the particularities of every dataset compared to conventional methods. However, their interpretability, privacy, and computational complexity limit their application in generative models. Only through additional research can it be achieved to the fullest extent that the AIs reach their potential for practical financial anomaly detection.

4. Uses

Anomaly detection with generative models has a wide range of applications across finance: Anomaly detection with generative models has a wide range of applications across finance:

- Banking – Identification of wrong credit card transactions account theft, and other fraudulent activities by indicating deviations from TRUE user activity patterns [11].
- Anti - money laundering – Put an end to instances of money laundering by monitoring money transfers with atypical sequences, abnormal routes, and other suspect data that show that illicit funds were exchanged [11].
- Risk modeling - increases risk detection regarding clients and investment portfolios by highlighting suspicious or fraudulent activities considered high risk [11].
- Surveillance Trade Monitor markets to find manipulation attempts, insider trading, and other violations by drawing statistical anomalies [11].
- The platform's security is automated adequately – monitor the employee access data, network traffic, and system activity to detect compromised credentials, cyber attacks, and insider attacks based on abnormalities [11].

Clickstream analysis – Find compromised accounts and fraudulent users, tracing them through anomaly patterns that may indicate bot - generated traffic or account takeovers [11].

5. Impact

A considerable proportion of financial wrongdoing would be mitigated if it became widespread to employ generative anomaly detection models worldwide. The UN calculates that globally, between 2% and 5% of GDP, from around 800 bln to 2 tln dollars, is the money laundered [12]. The increased ability to closely identify anomalies would result in many more of these illegal funds being detected and cut off by financial institutions before they could be used to harm various entities. Pointing out that undetected 1 % to 2% of the illicit capital flight means imposing $8 billion to $40 billion on the sectors of social need.

Generative models hold an edge over the traditional linear thresholding approaches. Hard thresholds often result in high false favorable rates when applied homogeneously, irrespective of the diversity requirements. In contrast, generative models train industry - specific models relying on the transactional data of each institution to learn the usual behavior patterns within each financial organization automatically [13]. As a result, anomaly detection gets more accurate, precise, and closer to the peculiarities of organizations that may skip incorrect fraud alerts.

Generally, generative models help reduce the rate of false positives and false negatives, which are common in anomaly detection [14]. This supports marking suspicious ones in the criminal financial realm while clearing the regular activity. Personalized targetted detecting could usher in a third paradigm, allowing a larger scale of illicit economic activity to be seized before possible harm is inflicted.

- Interpretability: The black - box nature of a majority of complex generative models creates issues in the matter of regulatory compliance. AI decisions must also be explainable to support a decision - making process that temporarily blocks a transaction.
- Privacy: The Important thing is detecting anomalies, but keeping the user data confidential is vital because of tightening data regulation.
- Complexity: Running and utilizing powerful yet highly resource - intensive generative models over large amounts of real - time financial info causes problems.

6. Scope

While generative models show immense promise for financial anomaly detection, further research is imperative to address critical challenges and realize their full potential. On the one hand, the generative models offer much potential for financial anomaly detection, but their realization requires urgent research to solve some critical issues that undoubtedly remain.

- Financial data - It has categorical features that show what type of business is being transacted, continuous values that represent the sums of money passing through different times, and temporal components that include timestamps of the events. Although nowadays there are various other methods of mining information from structured and integrated data (e. g., relational database or graph database), it is still a research topic of analyzing long - range dependencies in structured and integrated data types.
- Expertise knowledge - integrating first - hand knowledge into the model's architecture or even bringing it as a component for the trainer could add the dimensions for anomaly detection. For example, the fraud experts could counsel us on improving the existing database to identify fraud patterns that have not been detected.
- Data starving - The scarcity of a credible transaction dataset for learning is still the main obstacle, with few kinds of others. Supervised learning approaches and semi - supervised and really - few - shot classification techniques are essential ingredients in learning models from a limited number of anomalous data.
- Interpreting: AI models might behave differently than the directives set immediately, and there are few possibilities for supervising them. Explainable AI, as it applies to the professional finance domain, must come up with ways to function without requisite human intervention.
- Privacy - It must be emphasized that we can detect abnormal actions in complex IT environments without any additional risk of the whistleblowers` data being compromised because privacy is increasingly restricted. An aspect that cries for attention and 100% accuracy is personal data processing and algorithm designing methods.
- In - time live data streaming - Detecting and intercepting the unexpected data changes that value within such frequently changing financial streams may be tricky. For advanced AI models to be efficient in a real - time environment with varying concepts, flexibility is imperative that the advanced AI models can account for and adapt to the unstable concept of the environment.

The success of research concentrating on the solutions to the subsequent problems will help us take emotional intelligence from its ordinary academic level to accomplish things with real commercial value. Overcoming the novel financial shifts will depend on innovative approaches at a multi - disciplinary level, paying particular attention to the interpretability, security, and cyber protection of ML that will abet the unlimited prospects for better finance methods. This could be when the monetary institutions can no longer promptly detect suspicious patterns in the vast heterogeneous datasets. That stops fraud before it blows up, which in turn leads to preventing financial losses for both the banks and the clients.

7. Conclusion

Generative models are an advanced anomaly detection mechanism in dynamic financial data for learning normal data distribution. Methods such as autoencoders, GANs, normalizing flows, and so on have been successfully used to differentiate suspicious transactions that deviate from the given standard patterns. Despite all of that, the utilization of generative models requires overcoming several challenges. Interpretability is a central component of practical implementation in highly regulated sectors. Preserving privacy is, however, very relevant as regulations become stricter. Handling man various formats of data remains an issue. Additionally, a data scarcity anomaly influences the success of detection substantially. Significant investigations should be directed at perfecting generative models to adjust to the intricacies of financial data design. Developing interpretability, privacy, multidimensional data, and data scarcity solutions will take these generative models far from academic promises to real - world transformations. Such people have the potential to be the experts when it comes to detecting anomalies, which leads to a reliable way to spot illegal activities. This means financial crimes would essentially be wiped out, and highly specialized generative models would reach their utmost. Establishing their full power is a chance of thousandfold returns in the socio - economic area by eliminating the loss of billions to fraud, money laundering, etc.

References

[1] "Visual Analytics of Anomalous User Behaviors: A Survey | IEEE Journals & Magazine | IEEE Xplore, " *ieeexplore. ieee. org*. https: //ieeexplore. ieee. org/abstract/document/8950124/

[2] M. D. Flood, V. L. Lemieux, M. Varga, and B. L. William Wong, "The application of visual analytics to financial stability monitoring, " *Journal of Financial Stability*, vol.27, pp.180–197, Dec.2016, doi: https: //doi. org/10.1016/j. jfs.2016.01.006.

[3] S. Ahmad, A. Lavin, S. Purdy, and Z. Agha, "Unsupervised real - time anomaly detection for streaming data, " *Neurocomputing*, vol.262, pp.134–147, Nov.2017, doi: https: //doi. org/10.1016/j. neucom.2017.04.070.

[4] L. Jonsson, *Machine Learning - Based Bug Handling in Large - Scale Software Development*. Linköping University Electronic Press, 2018.

[5] H. GM, M. K. Gourisaria, M. Pandey, and S. S. Rautaray, "A comprehensive survey and analysis of generative models in machine learning," *Computer Science Review*, vol.38, p.100285, Nov.2020, doi: https: //doi. org/10.1016/j. cosrev.2020.100285.

[6] D. Gong *et al.,* "Memorizing Normality to Detect Anomaly: Memory - Augmented Deep Autoencoder for Unsupervised Anomaly Detection," *openaccess. thecvf. com*, 2019. http: //openaccess. thecvf. com/content_ICCV_2019/html/Gong_Memorizing_Normality_to_Detect_Anomaly_Memory - Augmented_Deep_Autoencoder_for_Unsupervised_ICCV_2019_paper. html.

[7] T. Schlegl, P. Seeböck, S. M. Waldstein, G. Langs, and U. Schmidt - Erfurth, "f - AnoGAN: Fast unsupervised anomaly detection with generative adversarial

networks, " *Medical Image Analysis*, vol.54, pp.30–44, May 2019, doi: https: //doi. org/10.1016/j. media.2019.01.010.

[8] B. Nachman and D. Shih, "Anomaly detection with density estimation, " *Physical Review D*, vol.101, no.7, Apr.2020, doi: https: //doi. org/10.1103/physrevd.101.075042.

[9] C. Liu, S. Ghosal, Z. Jiang, and S. Sarkar, "An unsupervised anomaly detection approach using energy - based spatiotemporal graphical modeling, " *Cyber - Physical Systems*, vol.3, no.1–4, pp.66–102, Oct.2017, doi: https: //doi. org/10.1080/23335777.2017.1386717.

[10] R. Gómez - Bombarelli *et al.,* "Automatic Chemical Design Using a Data - Driven Continuous Representation of Molecules, " *ACS Central Science*, vol.4, no.2, pp.268–276, Jan.2018, doi: https: //doi. org/10.1021/acscentsci.7b00572.

[11] SamanehSorournejad, Z. Zojaji, Atani, Reza Ebrahimi, and Monadjemi, Amir Hassan, "A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective, " *arXiv. org*, 2016. https: //arxiv. org/abs/1611.06439

[12] "Illicit Financial Flows to and from Developing Countries: 2005 - 2014 Global Financial Integrity E M B A R G O E D, " 2017.

[13] S. Latif *et al.,* "Leveraging Data Science to Combat COVID - 19: A Comprehensive Review, " *IEEE Transactions on Artificial Intelligence*, vol.1, no.1, pp.85–103, 2020, doi: https: //doi. org/10.1109/TAI.2020.3020521.

[14] D. Li, D. Chen, J. Goh, and S. Ng, "Anomaly Detection with Generative Adversarial Networks for Multivariate Time Series, " *arXiv. org*, Jan.15, 2019. https: //arxiv. org/abs/1809.04758