International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Synchronization of AI and Deep Learning for Credit Card Fraud Detection

[1]Dr. Irshad Nazeer, [2]Dr. KDV Prasad, [3]Dr. Promila Bahadur, [4]Dr. Varsha Bapat, [5]Dr. Kurian. M.J.

Submitted : 22/01/2023 **Accepted:** 27/03/2023

Abstract: At current scenario, more and more businesses are moving toward accepting credit card payments online, there is a growing demand for an efficient fraud detection solution that is able to send alerts in real time that can be acted upon. The banking and financial sector of a country is one of the most significant contributors to the growth and development of the economy of that country. In recent years, consumers have become increasingly reliant on credit and debit cards for all of their purchasing needs, whether they prefer to do their shopping online or in-store. Because of this, the number of people using bank cards has skyrocketed. As a result, the number of monetary exchanges completed with plastic has increased significantly. Customers & other organisations are all being put in a precarious position as a result of fraudulent actors in this situation. Internet banking has emerged as a significant channel for conducting business deals as a result of the widespread availability of more recent technological advancements. There is a significant trust and safety issue caused by fake activities and fraudulent transactions. This is a problem because fake banking activities and fraudulent transactions can be committed by anyone. Additionally, the proliferation of sophisticated frauds like virus infections, scams, and fake websites cause enormous losses due to fraudulent activities. These frauds are just some of the ways that fraudulent activities can result in enormous losses. All of these cons are examples of more sophisticated forms of fraud. This research makes three important contributions to the fight against fraudulent activity involving the use of credit cards.

Keywords*: Deep Learning, AI, Fraud Detection, Credit Card*

1. Introduction

The technique for detecting fraudulent activity in online banking makes use of the all-encompassing W2T method (Wei W et.al. 2013). Additionally, it offers multi-feature data of digital customers, which includes data on e-fund transactions, demographic data, credit card based transactions, and other types of data that are pertinent. These multiple facets of the data are sent to the data centre via the Internet. This data centre provides a platform that can be used to carry out a fraud recognition process for online banking (Taha A et.al., 2020). Customers and computer systems are treated as a single unit in online banking, which allows for the recognition and synchronisation of their respective relationships. During this W2T data cycle, one of the most important things to do is to predict fraudulent activity. Due to the fact that many customers do not frequently check their digital banking history, the system is unable to recognise and report fraudulent transactions immediately after the occurrence of the fraud. Because of this process, the likelihood of a successful recovery from a loss is significantly reduced (Claessens J et.al., 2002). In addition, every alert that is generated by the detection system needs to be manually investigated, which is a process that takes a lot of time.

The availability of low-cost infrastructure has contributed to the meteoric rise in Internet use over the past decade. This has resulted in an increasing preference for conducting business online, as evidenced by the rise of online banking system, mobile banking system, online credit as well as debit card transactions, and electronic wallets, among other examples. Credit cards are one of the most common methods used in the banking industry for conducting online transactions. The increasing number of people using credit cards and applying for credit to an increasing in the number of security risks and fraudulent activities. According to Wang et al.[1], the definition of fraud is the intentional commission of an act that is in violation of a law, rule, or policy with the purpose of obtaining an unauthorised financial benefit. Application fraud and transaction fraud are two distinct types of fraud that can be distinguished from one another (figure below).

[1]*Professor of MBA, Recognized Ph.D. Research Guide, Presidency Business School, Presidency College Re-accredited by NAAC with 'A+', Kempapura, Hebbal Bengaluru*
[2]*Assistant Professor (Research), Symbiosis Institute of Business Management (SIBM), Symbiosis International (Deemed University) (SIU) Off Bangalore Highway, Kothur Mandal Village: Mamidipally, Dist: Mahabubnagar, Hyderabad, Telangana*
[3]*Associate Professor, Department of Computer Science and Engineering, IET, Lucknow, Uttar Pradesh*
[4]*Associate Professor, Department of Electronic Science, PES'S Modern College of Arts, Science and Commerce, Pune, Maharashtra*
[5]*Associate Professor in Computer Applications, Baselios Poulose II Catholicos College, Piravom, Kerala*

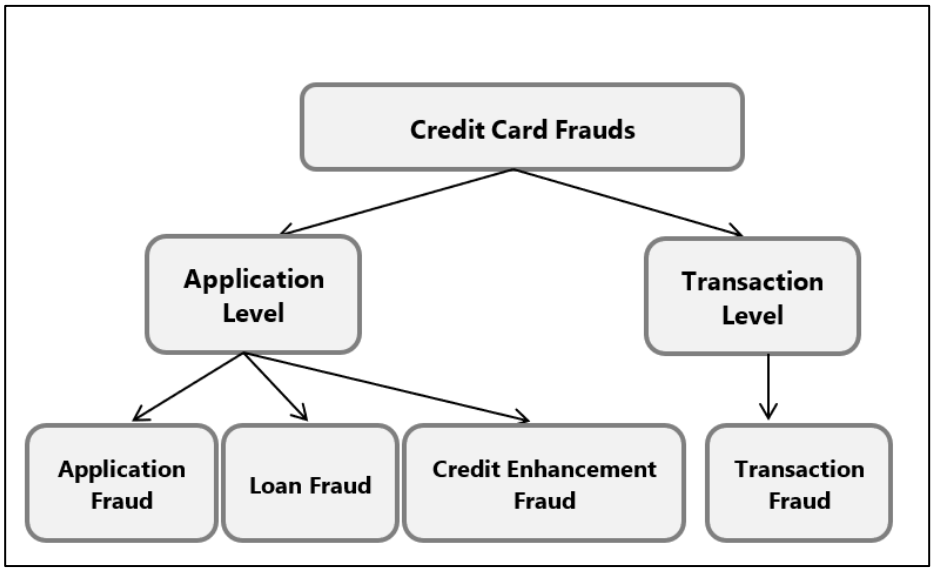

Fig. 1: Fraud Levels

When someone applies for a loan or a new credit card (CC) and opens an account in the name of another person, this type of fraud is known as application fraud. Application fraud is committed when the applicant uses forged or stolen documents. Voter identification cards, utility bills, and bank statements can all be stolen from a victim's home or taken from them in public by con artists who want to use the information for identity theft. Credit card application theft, loan forgery, and credit scoring fraud are the three main types of this type of fraud. When discussing fraudulent activities, the term "online fraud" is typically used. Transaction fraud occurs when a criminal makes unauthorised purchases with a stolen credit card by using the card number, the CVV number, and the expiration date. Credit card information is a prime target for fraudsters, who may use email, phone, or a phoney website to steal it. Card Not Present fraud, also known as CNP fraud, is the most well-known type of fraud that can occur during online transactions because they are completed in a fraction of a second. Therefore, phishing, counterfeiting, identity theft, and skimming fraud are the most common types of credit card scams (Revathi P, 2019). As a result of these scams, both individuals and the government have suffered significant financial losses. Numerous industries, including banking, insurance, telecommunications, and others, are susceptible to fraud.

2. Review Literature

When someone applies for a loan or a new more facility based credit card (CC) and opens an account in the name of another known person, they have committed application fraud. Application fraud occurs when an applicant uses false information or stolen credentials to gain an advantage in the application process. Voter ID cards, utility bills, and bank statements are all items that identity thieves can use to create a false identity by simply stealing them from a person's home or a public location. The information is being stolen for an ulterior motive.

There are three distinct types of fraudulent activity here: applications for credit cards, loans, and credit enhancements. Online fraud refers to any type of fraudulent online transaction. Without actually possessing the credit card itself, criminals commit transaction fraud when they make unauthorised purchases using stolen the credit card related details such as the card numbers, the unique CVV numbers, and the expiration date. When a fraudster uses a stolen the credit card, they are committing "possession fraud." Credit card information can be stolen in a number of ways, including over the phone, online, or via a phoney website. Among these are the internet and the telephone. Due to the lightning-fast completion time of online transactions, Card Not Present fraud, also known as CNP fraud, has become the most well-known form of fraud that can occur during these types of transactions. This is due to the fact that the card is not present during the actual completion of the transaction. Therefore, phishing, counterfeiting, identity theft, and skimming are the most frequent forms of credit card fraud (Revathi P, 2019). Because of these cons, both private citizens and the government have lost substantial amounts of money. In addition to the financial and insurance industries, the telecommunications industry is also vulnerable to fraud.

Role of deep learning & AI in Fraud Detection

Deep learning models may be more effective at reducing the false positive rate (FPR) than more conventional machine learning approaches, which could mean less customer offensive word, fraudulent charges, and fraud. Explosion in the number of people using internet & new distribution channels for online activities have given rise to an increase in the number of opportunities for fraudulent activity and abuse as electronic payment

methods become more widely used. In order to better understand the magnitude and complexity of the issue, we have provided this illustration. Given the prevalence of identity theft, account takeover, and stolen credit cards in today's society, how can we verify the legitimacy of new and returning customers making purchases or requesting refunds (online or in-store)?

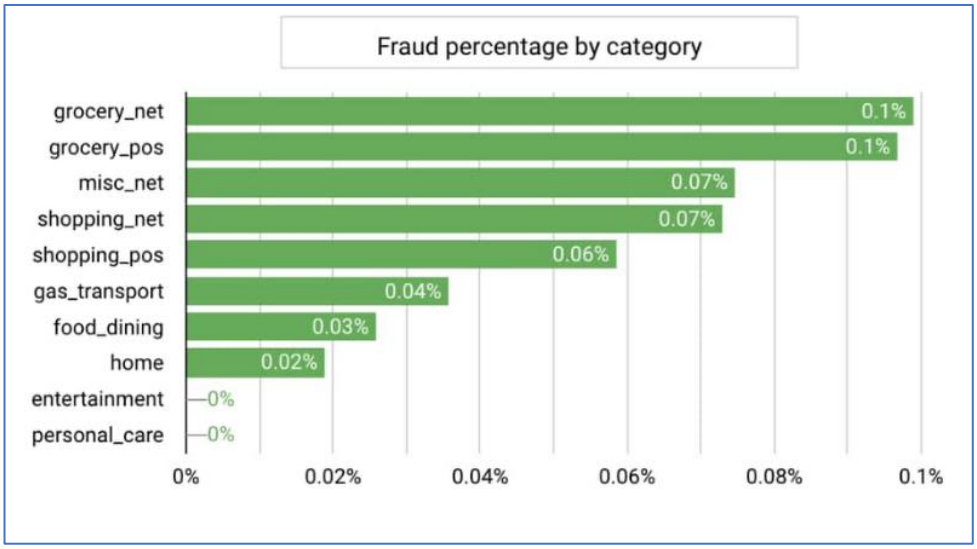

Fig. 2: Fraud percentage by category

Although the identification of fraudulent activity is one application of anomaly detection, the more general field of machine learning and artificial intelligence (AI) is plagued by ambiguity in the definition of an anomaly (or outlier), as well as challenges in verifying and monitoring results. Supervised learning, wherein we learn from an existing body of labelled or verified data, could be used to build the detection model. Without sufficient examples or labels, however, most anomaly detection techniques would fall into the category of unsupervised or semi-supervised learning problems.

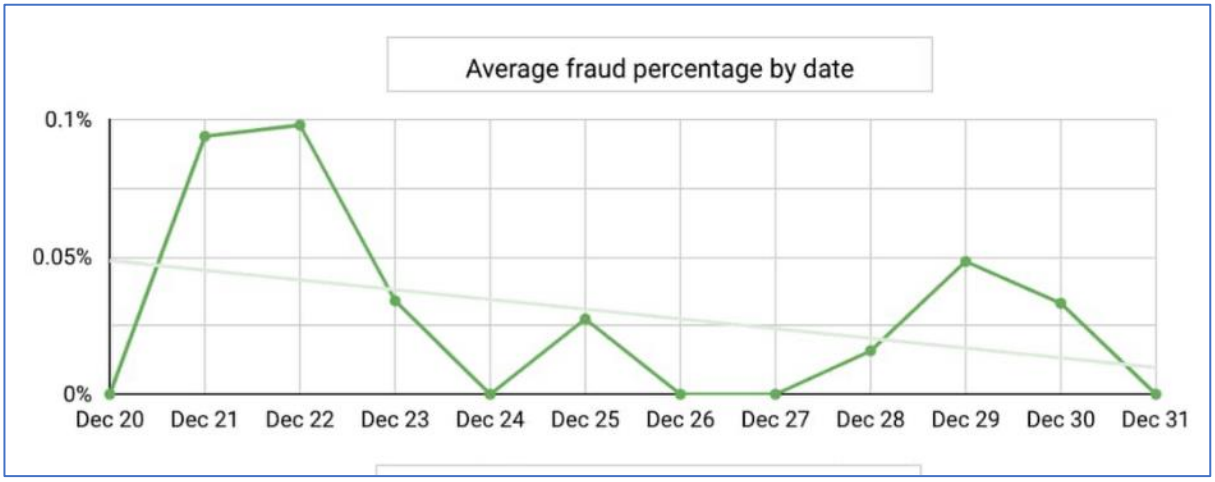

Fig. 3: Avg. fraud percentage by date

In addition to the massive amounts of data that need to be processed and the complexity of transactions related to finance, fraud detection faces a few other challenges, which will now be summarised. In this post, we examine a few topics related to the field of deep learning & ANN based solutions for detecting fraudulent activity in e-transactions.

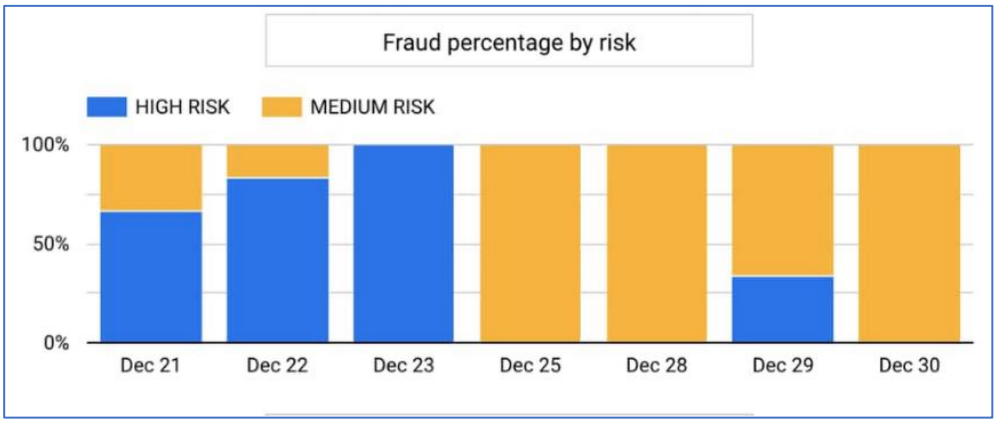

Fig. 4: Fraud percentage by risk

As is the case with a great number of other machine learning challenges, there is the possibility that deep learning (DL) approaches will result in improved performance. The benefits of DL include a significantly reduced requirement for feature engineering, as well as improved learning alonwith good performance so that the more & more data can be collected.

Fraudulent transactions at merchant

merchant	category	fraudulent_amt ▼	num of fraudulent ...
fraud_Okuneva, Schne...	shopping_pos	1.3K	1
fraud_Willms, Kris and...	shopping_pos	1K	1
fraud_Mosciski, Ziem...	shopping_net	1K	1
fraud_Predovic Inc	shopping_net	997.8	1
fraud_Zboncak, Rowe ...	shopping_net	981.2	1
	Grand total	**10K**	**19**

Fig. 5: Fraud transactions at merchant

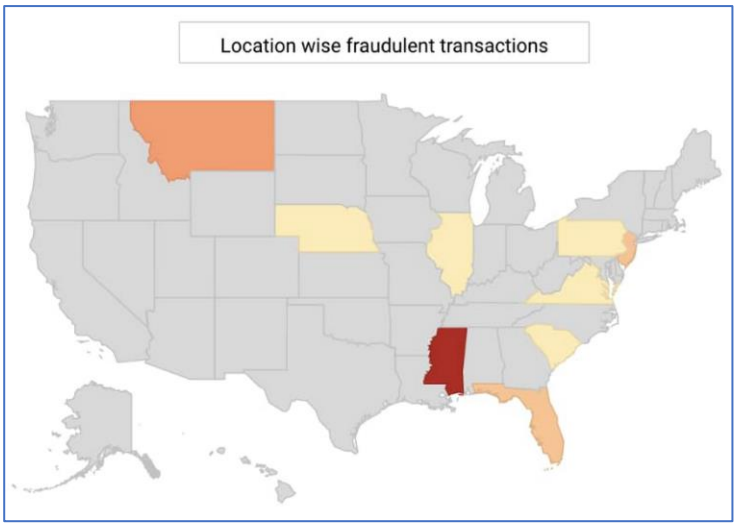

Fig. 6: Location wise fraud transactions

What difficulties exist in detecting credit card fraud?

From the preceding analysis, it is clear that having access to a large amount of real-time and historical data about the customer and the transactions is crucial for resolving the majority of problems associated with fraud and abuse detection. This data includes the shopper's demographics, their connections to other customers, where and how they've shopped before, and whether or not they've returned anything. The issue then becomes determining when and how to know for sure that stolen credit card details were used to make the purchase. The fact that conventional approaches to fraud detection require

extensive data pre-processing and engineering work is another relevant topic for discussion in this setting. Specifically,

- The high dimensionality of the feature space makes the task of building a fraud detection model challenging from a machine learning perspective (Bogaerts et. al. 2021). A huge number of input attributes or it's types are obtained after pre-processing, quantization, and feature embeddings. These characteristics are derived from the ongoing transaction in addition to attributes derived from the customer's profile and all related prior transactions and events.

- As an example of an unbalanced machine learning problem, the fact that only a tiny fraction (much less than 1%) of transactions are fraudulent presents a significant obstacle to financial fraud detection. Thus, it is challenging to master the art of identifying fraud cases with high accuracy while simultaneously reducing the false positive rate (FPR). Boosting the FPR is as simple as focusing on a higher fraud detection (or true positive) rate. If a legitimate transaction is incorrectly identified as fraudulent (i.e., a false positive), it will not only result in a drop in revenue but also in customer dissatisfaction and the subsequent involvement of customer service (i.e., an increase in labour cost) in order to rectify the situation and appease the customer's hurt feelings. A higher FPR in a detection model will result in an increase in the rate at which customers are insulted, which could lead to the loss of some legitimate customers. Of course, not every customer who insults you calls your office.

- The data labelling problem, i.e. deciding whether or not a transaction was fraudulent, is another obstacle to developing a fraud detection model.

- Another problem with data labelling is the wide variety of fraud schemes that can be employed. In addition, fraudsters frequently adopt novel approaches. Therefore, such examples of possible fraud or abuse may be absent from our historical database. An unsupervised or semi-supervised anomaly detection model could be useful in such circumstances.

- In order to convert a continuous "fraud score" or "fraud probability" from a fraud detection model for a given transaction into a final decision, it is common practise to select some thresholds.

Data pre-processing and feature embeddings are still required for a deep learning-based solution, but less feature engineering is required compared to traditional approaches. Due to their complex nature and the longer time it takes to train or construct them, deep learning detection models struggle to scale in production to handle high volumes of concurrent users and transactions.

3. Deep Learning-Based Solutions

To that end, this blog post will elaborate on several methods for detecting fraud, including encoder-decoder based structure, the generative adversarial networks & also other semi-supervised methods, as well as supervised methods & transfer learning.

4. Encoder-Decoder Structure or Auto-Encoder

When reframed as an unsupervised or self-supervised anomaly detection problem, fraud detection may be amenable to an auto-encoder (AE). The high volume of unlabeled data, along with the challenges and unknowns of labelling data, contribute to this (fraud vs. normal).

- Learning a compressed representation of data or a generative model of "normal" data is the primary goal of auto-encoders. Next, we can identify "abnormal" inputs by seeing if the reconstruction error is larger than a predetermined limit. In AE, the input features are first compressed into a bottleneck or latent space vector by the encoder, and then the input is re-created by the decoder using the compressed latent vector.

- The output will likely vary from the input when abnormal data is used as the input because AE learns a compressed generating model from a large body of normal data.

- Because AE learns the model from a large set of normal data, it produces these results. The reconstruction error, which is the difference between the input and the output, can be used as a fraud score in scientific investigations.

There are many different auto-encoder methods, but the variational auto-encoder (also known as VAE) is one of the ones that has the most potential (Kingma et. al., 2019).

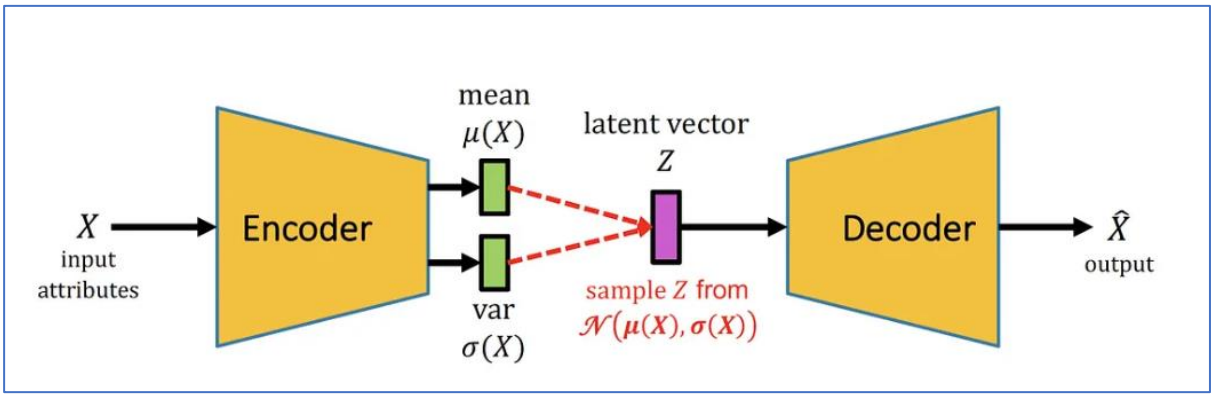

Fig. 7: Construction of a Variational Auto-Encoder (VAE). In other words, its encoding and decoding mechanisms are based on probability theory. In order to control the output, the low-dimensional random latent vector Z is learned by the model to reconstruct the input.

The probabilistic generative extension that is VAE is an extension that is added to the initial AE structure. The mean and standard deviation are the two compressed vectors that are estimated by the encoder of the VAE. When put together, they depict the data's probabilistic distribution in the reduced dimensionality. By sampling from the distribution, the latent vector Z produces an output that is statistically very "similar" to the input X when the data is normal and consistent with the vast majority of data seen during the VAE's training process.

Generative adversarial network (GAN)

While VAE relies on an explicit probability density estimation, GANs are an extension that eliminates the need for it. The generator takes a compact latent space vector at random and uses it to create synthetic or fake data that closely resembles the real thing. The generator is tasked with producing synthetic or fake data that is as close to the real thing as possible so that the discriminator can train to tell the difference. The data's distribution and properties are set by the generator's latent space vector (Goodfellow et.al. 2016).

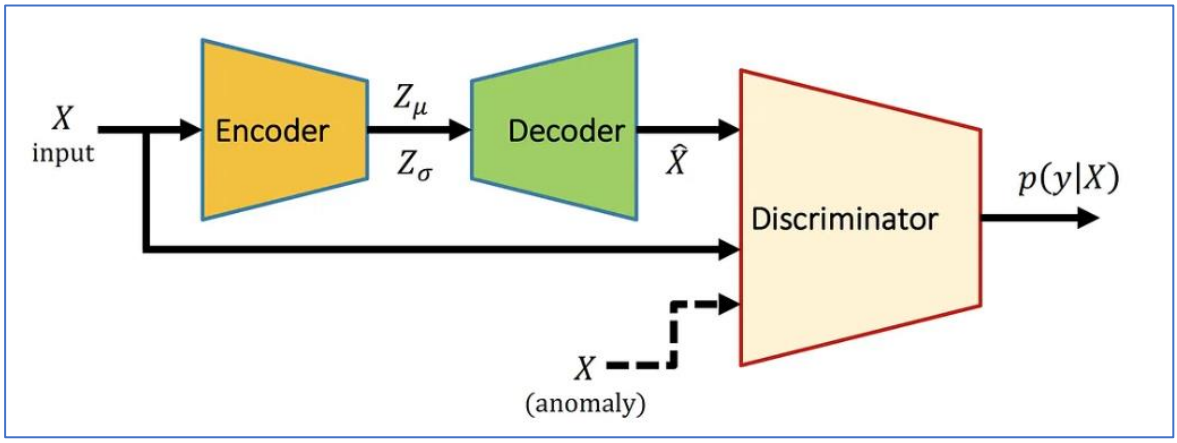

Fig. 8: Variational Auto-Encoder Construction (VAE). Probability theory governs its encoding and decoding. The model reconstructs input using the low-dimensional random latent vector Z to control output (Kimura, et al., 2020).

We've established that in GAN, the decoder part of a VAE structure is often used as the data generator. By learning both the generator and the discriminator parts of the problem at the same time, GAN challenges VAE and helps improve its performance. VAE is a data-generation unsupervised learning task.

Deep Learning is a supervised approach to detecting fraud.

An approach to fraud detection that is based on supervised deep learning may be able to provide high accuracy and performance with sufficient historical labelled data sets. In this case, we are very sure of the dates and times of the chargebacks, fraudulent transactions, customer insult events, return abuse cases, and so on that were based on the samples of data we analysed. It is possible that a supervised deep learning-based approach can achieve this level of precision and efficiency.

Due to the fact that there are numerous distinct variety of input based features or attributes (such as point data, in addition to event data and sequential data), the process of feature extraction can be approached from two different perspectives:

1. One, we can use a ConvNet or RNN deep learning model with sequential data and event time series. Feature extraction will be handled mechanically by the deep learning model in this setup. This is an illustration of a full-stack machine learning architecture.
2. In addition to information pertaining a variety of pertinent attributes or features from sequential historical information as well as information pertaining to the currently concluded networks or interactions. After that, we would be able to use a deep learning model to incorporate all of these extracted quantitative features. Deep learning models perform more effectively on high-dimensional data when compared to more conventional machine learning methods.
3. Third, over-sampling the fraud samples and under-sampling the normal samples can be very helpful when dealing with the issue of an unevenly distributed training dataset.

Transfer learning

If we have a DL-based model that was trained on a large dataset for a fraud detection problem or application, we can use it for a different problem or application that uses a smaller dataset by simply adjusting the model's parameters. This process is known as "domain adaptation," transfer learning, or simply learning that is taken from one setting and applied to another.

Let's pretend that our other, brand-new fraud detection problem also makes use of the aforementioned attributes in its input data, but lacks sufficient training data. We'll be able to get in a bit more practise or fine-tune work sooner. The time spent training can then be devoted to the new task at hand. As a result, we are able to improve performance in a problem (sometimes called the "target domain") where there is insufficient training data by generalising the experience and transferring the knowledge gained from solving a different problem (the "source domain") (Lebichot et. al., 2020)

- We can use transfer learning in a variety of ways, ranging from unsupervised to supervised methods, and it has many applications. Given that the initial layers of a deep learning model are the ones responsible for performing the task of feature extraction, one approach would be to keep the initial layers of the original pre-trained deep learning model in their original state and only fine-tune or adapt the top layers (i.e., layers that are close to the output) by making use of our new, relatively small dataset.
- Transfer learning can also be useful in the process of data augmentation, which involves the use of synthetic data, and this is especially true for the analysis of time series data or sequential data. It is important to keep in mind that anomaly events in real life are extremely rare, and as a result, the process of training could benefit from the generation of synthetic anomalies.

5. Findings of the Study

False positive rate (FPR) reduction using deep learning models may lead to less customer insult, chargebacks, and fraud as compared to more traditional machine learning approaches. It's important to remember that, when dealing with a large-scale and competitive e-commerce, even a small improvement in FPR and chargeback rates (say, a reduction of 5 to 10 percent) can have a significant impact on the bottom line.

Having the ability to learn is a major benefit of deep learning-based models. This means that as our database grows larger, these models will be able to automatically extract higher-level features, learn more nuanced detection models, and boost their performance with larger, more comprehensive training datasets.

A large number of the real-world uses for deep learning involve providing comprehensive answers to extremely difficult problems. This means that the curse of dimensionality and the difficulty of extracting useful features are reduced.

6. Conclusion

The current topic of how to best protect against and investigate credit card fraud is one that has long piqued the interest of, and prompted investment from, financial institutions. Credit card fraud is a crime that is increasing at an alarming rate and causes a staggering amount of financial damage every year around the world. Conventional methods of preventing and detecting fraud are less adaptable in such a setting. In this paper, we cover not only the proposed framework but also a range of adaptive strategies for avoiding fraud. Using three distinct layers of verification strategies, the framework presented a systematic approach to fraud prevention and detection at all levels of transactions. Successfully utilising threshold values and historical fraud patterns, these techniques have been used to identify potentially fraudulent transactions and applications (white & blacklist). Credit card fraud was also preserved and reduced in the early stages of the card's life cycle. In addition, we identified and investigated cases of fraud within the dataset.

References

[1] Achituve I, Kraus S, Goldberger J, “Interpretable Online Banking Fraud Detection Based on Hierarchical Attention Mechanism”, In proceedings of 2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP), pp.1-6, October 2019.

[2] Bogaerts, B., Bontempi, G., Geurts, P., Harley, N., Lebichot, B., Lenaerts, T., & Louppe, G. (2021). Artificial Intelligence and Machine Learning.

[3] Claessens J, Dem V, De Cock D, Preneel B, Vandewalle J, "On the security of today's online electronic banking systems", Computers & Security, vol.21, no.3, pp.253-65, June 2002.

[4] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press.

[5] Dembla, N., & Arya, M. K. (2019). Effect of Machine Learning in E- Commerce. Kaav International Journal of Economics, Commerce & Business Management, 6(1), 298-305.

[6] Kingma, D. P., & Welling, M. (2019). An introduction to variational autoencoders. *Foundations and Trends® in Machine Learning*, *12*(4), 307-392.

[7] Lebichot, B., Le Borgne, Y. A., He-Guelton, L., Oblé, F., & Bontempi, G. (2020). Deep-learning domain adaptation techniques for credit cards fraud detection. In *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* (pp. 78-88). Springer International Publishing.

[8] Lebichot, B., & Saerens, M. (2020). An experimental study of graph-based semi-supervised classification with additional node information. *Knowledge and Information Systems*, *62*(11), 4337-4371.

[9] Taha A and Malebary S J, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine", IEEE Access, vol.8, pp.25579-87, February 2020.

[10] Revathi P, "Digital Banking Challenges and Opportunities in India", EPRA International Journal of Economic and Business Review, vol.7, no.12, pp.20-3, 2019.

[11] Srividya, R., & V, L. (2018). Artificial Intelligence in Hospitals. National Journal of Arts, Commerce & Scientific Research Review, 6(1), 335-338.

[12] Srivastava, A., Srivastava, P., & Chaudhary, A. (2022). DigitaL Fraud (1st ed., pp. 11-18). Kaav Publications. https://www.kaavpublications.org/cpabstracts/digital-fraud.

[13] Sivakumar, N., Balasubramanian, R.: Fraud detection in credit card transactions: classification, risks and prevention techniques. International Journal of Computer Science and Information Technologies 6(2) (2015)

[14] Wei W, Li J, Cao L, Ou Y, Chen J, "Effective detection of sophisticated online banking fraud on extremely imbalanced data", World Wide Web, vol.16, no.4, pp.449-75, July 2013.

[15] Wang, J.H., Liao, Y.L., Tsai, T.m., Hung, G.: Technology-based financial frauds in taiwan: issues and approaches. In: Systems, Man and Cybernetics, 2006. SMC'06. IEEE International Conference on. IEEE (2006)

[16] https://cloud.google.com/blog/products/data-analytics/how-to-build-a-fraud-detection-solution

[17] https://medium.com/walmartglobaltech/deep-learning-for-fraud-detection-in-retail-transactions-564d31e5d1a3#:~:text=Deep%20learning%20models%20could%20help,to%20traditional%20machine%20learning%20methods.