# Literature Review

Most classification algorithms, which can be broadly classified as machine learning and artificial intelligence systems, are frequently not used by financial institutions due to stricter regulatory Committee requirements that support the use of parametric models for a simple and clear interpretation of the results. Despite the regulatory preference for adopting the statistical framework. (Ewanchuk and Frei 2019), a growing body of evidence supports the employment of sophisticated models in credit risk assessment (Leo et al. 2019).

(Alaka 2017), gives a comprehensive assessment of tool selection for analysing bankruptcy prediction models and address more advanced models for credit risk calculation.

(Chakraborty and Joseph 2017) advocate the use of a machine learning model to detect financial distress using balance sheet information, and their study concludes that the machine learning model outperforms the logistic regression model, which is the preferred classical approach of financial institutions.

(Khandani et al. 2010), used state-of-the-art non-parametric machine learning models to predict consumer credit risk default by combining transaction and credit unit data. Their research shows that machine learning techniques may increase risk prediction more than traditional statistical approaches and that any subsequent lender loss can significantly be improved.

(Albanesi and Vamossy 2019), used a deep learning strategy based on a neural network and gradient boosting for high-dimensional data to forecast customer risk default. Their work outperforms logistic regression models in terms of performance and adaptability to the aggregate behaviour of default risk.

(Bacham and Zhao 2017), compared the performance of machine learning models to industry-developed algorithms such as Moody's proprietary algorithm and proposed a 2-3 percentage point improvement in machine learning model performance. Although credit-behavior-related factors boost the discriminating strength of the studied models, their approach is somewhat challenging to associate with the underlying company characteristics in forecasting credit risk default.

In estimating credit risk default of small-medium firms, (Fantazzini and Figini 2009) suggested a non-parametric technique based on random survival forests. The performance comparison of their proposed model with the traditional logistic regression model reveals a weak relationship of performance between training and testing samples, implying an over-fitting problem, which is primarily due to contrasting logistic regression testing sample performance better than their proposed random survival models.

Several more research, including (Kruppa 2013; Yuan 2015, Barboza 2017; Ampountolas 2021 and Addo 2018); demonstrate that machine learning outperforms any other statistical technique for credit risk prediction.

The literature on the non-statistical model frequently argues that the discrepancy between the expectation of the averaged forecasts and truth is dependent on the bias of contributing models as well as their weights. The underlying assumption for statistical model averaging literature, however, is that there is no bias, therefore their contribution is frequently less interesting (Burnham and Anderson 2002).

Reducing bias is frequently highlighted as the major motivation for model averaging in many of the literature publications, particularly those linked to process models (Solomon et al. 2007; Gibbons et al. 2008; and Dietze 2017).

Weights are quadratic in terms rather than linear due to the nature of predictions, since knowing completely the correct approach to calculating weights is essential. (Breiman 1997) adds several advantages to the model averaging technique. Apart from the inaccuracy of the estimate, obtaining a decent estimator for the optimal weight in the first place is an open problem, and there is no such closed solution accessible, even in the case of linear models (Liang et al. 2011).

The literature generally supports parametric, non-parametric, and ensemble model-averaging methodologies. Model averaging appears to be of importance for reducing prediction error as well as better reflecting model selection uncertainty (Buckland 1997; Madigan and Raftery 1994).

(Claeskens 2016) assumed that estimated model weights are beneficial in general since they are bias-free and have identical prediction variance, but this does not indicate that calculated equal weights are preferable. This field of study, to our knowledge, might be expanded by offering numerous suggestions for selecting weights, and the methodological approach outlined in this work is an effort in this direction to improve model predictive performance.

It is critical to understand that machines are not born intelligent. In general, supervised learning algorithms are trained to be clever by employing information gained from previous data. As a result, the historical data and learning algorithms are likely to prejudice the robots. The bias might render a computer incapable of dealing with undesirable scenarios for which it has not previously been taught. A human, on the other hand, can deal with such a problem, either by utilising his or her own abilities or by collaborating with others. So, should we employ machine intelligence to approve credit cards automatically? Instead of full automation, we believe that machine intelligence may be leveraged to aid people in the credit card acceptance process. (Mehrabi, N. 2019).

Existing machine learning approaches generally assist the decision-making process by predicting or recommending the output of an observation. However, it is quite often reported in the literature that the end-users are sceptical about the trustworthiness of such a recommendation. It may be more prevalent in sensitive areas like finance, healthcare etc. Significantly, it is not possible for a machine to correctly recommend the approval of all credit card applications. Even if a machine is tested to be sufficiently accurate, unexpected behaviour could be possible in a real banking environment. The availability of recommendation confidence can help in such circumstances. (Toreini, E. 2020)

According to the credit card statistics presented by the Central Bank of Ireland in April 2022, it is noteworthy how the use of credit cards has increased compared to the previous year, due to the recent pandemic affecting consumer behaviour. Overtime banks build an extensive customer database that can be analysed to evaluate the bank’s performance and make strategic decisions based on customers’ experience behaviour, this is a process that is still improving to find better accuracy and precise model, and this is the reason why banks are always working on their customer experience, and adapting to changes and new trends; not all customers behave similarly regarding financial behaviour; therefore, a different treatment should be given to those who meet certainly profitable, this is becoming increasingly challenging for banks, especially for the credibility that a new customer must build by proving to the financial institution that they can be responsible with the debt acquired, at the same time the system will assign a score to the customer according to how the client managed the debt, as a bank record for future applications.

There are different studies about credit card prediction, however, it’s a topic that is still improving to achieve the ideal performance for Financial Institutions, this makes it a trending topic since the fact that it will always look to develop new technologies. The research suggests using machine intelligence to automatize processes, nevertheless, this procedure is still depending on a final decision from a human to analyse and determine if the applicant is suitable for the financial portfolio, which means the machine cannot take the decision to trust or not based on the result, there are many factors which can help to consider or refused the applicant.

These are some cases of credit cards that are related to electronic fraud, either directly or indirectly.

a) Credit Card Fraud: Credit cards, both virtual and real, are used to purchase supplies and services.

Virtual cards are used to commit fraud online, typically through the internet or phone, by getting credit card information illegally. Physical cards are used to commit fraud offline; the attacker must take the credit card.

b) Bankruptcy Fraud: Using a credit card while absent; concealing him; or engaging in other activities that cheat his creditors. Because of its intricacy, this form of fraud is difficult to foresee. (L. Delamaire, and J. Pointon. 2009).

c) Computer intrusion: the act of pushing one's way in getting unauthorised access to information with the intent of subverting the protection and detection mechanism.

d) Theft fraud / Counterfeit fraud: theft fraud is the use of a credit card without the owner's authorization, which may be checked as soon as the owner reports it to his financial institution. While credit card fraud offers the greatest risk, simply the credit card's data are necessary. (K. Chaudhary and B. Mallick, 2012).

e) Telecommunications: the use of telecommunication services to perpetrate various sorts of fraud is constantly changing; businesses, communication service providers, and consumers are all victi  Credit Card Fraudsters

There are many credit card fraudsters; some of them are listed below. (J. Akhilomen. 2013)

a) Credit Card Information Buyers: These are a group of fraudsters with limited IT abilities who obtained stolen or hacked credit card information from an illicit website in order to purchase goods and services digitally.

b) Black Hat Hackers: They are essentially fraudsters who get unauthorised access for malevolent motives, particularly for personal gain; they employ the "pre-hacking stage" procedure, which includes targeting, research, information gathering, and concluding the attack.

c) Physical credit card thief: This category includes fraudsters who steal credit cards for illicit reasons. This is the simplest method for a fraudster to obtain the cardholder's information without investing in contemporary technology.ms of this fraud. (K. Chaudhary and B. Mallick, 2012).

* Credit card fraud detection techniques.

Fraud detection techniques are classified into two broad categories: fraud analysis (misuse detection) and user behaviour analysis (anomaly detection). (S. Maes K. Tuyls and B. Manderick 2002).

In anomaly detection, typical user behaviour is utilised to create a normal profile of the user, which is then used to check for large deviations from the normal user profile, which are deemed fraudulent transactions. This is an unsupervised pattern based on user account profile behaviour because each user, as well as the fraudsters, has their unique profile behaviour.

Incoming transactions are compared to a categorised supervised model of a known fraudulent transaction, which is programmed into a pattern to detect genuine and fraudulent transactions. To determine if a transaction is real or fraudulent, historical data is utilised to develop a categorization model. (S. Maes K. Tuyls and B. Manderick 2002). Briefly describes some of the most recent credit card fraud detection systems.

A diagram of a model

Description automatically generated with low confidence

* Clustering Methods.

Suggests two clustering techniques: peer group analysis and break point analysis. (R. Bolton, & D. Hand. 2002), Peer group analysis refers to earlier accounts that were acting similarly but suddenly began behaving noticeably differently; the system finds these accounts and flags them as suspicious. While break point analysis takes a different technique, when a large quantity is transferred, an account might be identified as suspicious and examined.

* HMM (Hidden Markov Model).

Hidden Markov Model is a limited set of states, each with its own probability distribution. To administrate transition between these states, a set of probabilities known as transition probability is employed (A. Singh and D. Narayan. 2012). The central concept is to construct a multilayer model of programme behaviour based on both HMM and enumerating approaches for anomaly detection (T. Lane 1997). This methodology (HMM) does not require a fraud signature and may successfully identify fraud based just on the credit card owner's spending behaviour. The HMM examines the cardholder's spending habits based on a threshold value of high (h), medium (m), or low (l). This threshold value is dynamically determined by the clustering algorithm of each cardholder's personal expenditure routine.

The most important advantage of the HMM-based technique is that it considerably minimises the number of valid transactions (false positives) identified as suspicious by the fraud detection system.

* SVM stands for Support Vector Machine.

This technique is appropriate for detecting credit card fraud since it just requires two classes: valid and fraudulent. SVM attempts to compute an optional hyper lane that separates the sample of the two classes (D. Meyer 2012). SVMs are supervised learning models that use learning algorithms to analyse and recognise patterns for classification and regression tasks (N. Cristianini and J. Shawe-Taylor. 2000). Kernel representation and margin optimisation are two critical components of SVM. The optimal kernel for any given problem is a massive research challenge; speed and size (large training set), which decreases the demand computational for testing poses a key restriction to SVM.

* The Decision Tree.

The decision tree is a diagram that depicts the potential consequences of a set of connected selections. It is used to create an algorithm that accurately predicts the optimal option. A decision tree may also be used to develop automated prediction models with many applications in data mining, machine learning, and so on. This approach can consider an item observation to forecast the value of that element. The advantage of this strategy is that it adds additional choices to an existing tree, is simple to grasp, and requires no data preparation. However, this approach has drawbacks in that it might grow very complicated and verify each operation one by one for better accuracy; several trees are frequently employed simultaneously in the ensemble method. (W. Fan,, M.Miller, S. Stolfo. 2001).

* Algorithm Genetic.

Genetic algorithms are heuristic search and optimisation methods that are encouraged by natural selection and belong to the wider family of evolutionary algorithm methods; these evolutionary algorithms have a propensity to get better solutions as time progresses. The challenge of fraud detection is a classification problem; GA has been applied in credit card fraud detection to minimise the amount of transactions incorrectly categorised. (E. Duman, and H. M. Ozcelik 2011). GA is effective in detecting credit card fraud due to the ease with which programming languages may be implemented. It does, however, have a memory limitation and is time demanding.

* The Artificial Neural Network.

This simulates how the human brain operates in certain circumstances, in order to accomplish the operations of nodes known as neurons. Neurons are computing units that process incoming data and generate output data. (E. Ngai, Y. Hu., Y. Wong 2011). A neural network is an interconnected network of nodes that reflect the linking functions of the human brain. (S. Ghosh, and D. L. Reilly 1994). ANN are nonlinear statistical data modelling tools that may build supervised/unsupervised learning patterns by modelling the complicated link between input and output. ANN is a random function approximation tool that can learn by viewing datasets. In ANN, the terms "training" and "recognition" are frequently used. In the ANN supervised training approach, sample data from both fraudulent and non-fraudulent transactions are utilised to develop models in fraud detection systems. (T. Guo, and L. Gui-Yang 2008).

A picture containing text, screenshot, diagram, font

Description automatically generated

* Machine learning approaches in behavioural scoring.

The field of credit scoring has become a broadly investigated subject by researchers and the financial industry, with numerous models having been proposed and created utilizing measurable methodologies, and Linear Discriminant Analysis. Because of the financial crisis, the Basel Committee on Banking Supervision demanded all banks apply thorough credit assessment models in their frameworks while conceding a loan to an individual customer or a company. Appropriately, research has shown that Artificial Intelligence (AI) procedures (e.g., neural networks, SVM, and RF) can be a decent exchange for measurable methodologies in building credit scoring models. (Bellotti T, Crook J. 2009).

Credit card transaction data has grown dramatically in recent years. As a result, using typical mathematical and statistical models for such issues is difficult. Nowadays, the notion of scoring models is well recognized, which provide a specific score or assessment to applicants seeking credit; feature choices created from customer transactions assist to identify which items are available to the suitable client.

There are two types of credit scoring: application credit scoring, in which a score is used to make a judgement on a new credit application, and behavioural credit scoring, in which the score is used to address current clients after they have been granted a loan. Banks use behavioural scoring to guide lending decisions in credit limit management strategies, debt collection and recovery, retaining future profitable customers, predicting accounts likely to close or settle early, offering new financial products and interest rates, managing inactive accounts, optimising telemarketing operations, and predicting fraudulent activity, the number of risk payments, and future risk of payment.

* Recurrent and LSTM Neural Networks.

RNNs (recurrent neural networks) are a subset of supervised machine learning models. They are composed of a series of cells with hidden states and non-linear dynamics. RNNs are typically applied to time series data, such as voice recognition, unsupervised anomaly detection, and automatic translation. In economics, LSTM is used as an alternative to the ARIMA model to forecast time series data. (Malhotra P. 2015).

Because credit card transactional data is temporal in nature, RNNs should be used instead of other types such as fully connected or convolutional neural networks.

This is one of the models that is more commonly used nowadays for financial risk prediction analysis. It is important to highlight that this model is widely used in economics for predicting, implying that it is used in conjunction with recognition and unsupervised learning.