Journal of Theoretical and Applied Information Technology
15th June 2019. Vol.97. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FRAUD PREDICTION IN BANK CREDIT ADMINISTRATION: A SYSTEMATIC LITERATURE REVIEW

[1] IBUKUN EWEOYA, [1, 2]AYODELE ADEBIYI A., [1]AMBROSE AZETA, [3]OKESOLA OLATUNJI

[1]Researcher, [2]Professor. Covenant University, Department of Computer and Information Sciences, Ota, Nigeria

[2]Professor. Landmark University, Department of Computer Science Omu-Aran, Nigeria

[3]Professor. Technical University, Department of Computational Sciences, Ibadan, Nigeria

E-mail: [1] ibukun.eweoya, ayo.adebiyi, ambrose.azeta{@covenantuniversity.edu.ng}, [3]olatunjiokesola@tech-u.edu.ng

ABSTRACT

Any business or organization that intends to be far from bankruptcy or crime strives daily to ensure crime perpetration does not occur in the organization unabated. Traditional methods of fraud detection in credit administration are available but limited in capacity to check current sophistication in fraud perpetration; those approaches did not offer the best for time-consumption and efficiency; also, frauds are better predicted rather than a detection after the deal is done. This work presents an extensive review of literature and related works in fraud prediction in credit administration. The primary focus of this research work is to identify and dwell on the major concepts and techniques used for financial fraud prediction in credit administration as well as related works that have been done in this domain of study; while the work recommends the ensemble approach as a better alternative in this domain. The existing systematic literature reviews in this domain are not in the context of credit fraud prediction alone.

Keywords: *Fraud, Supervised learning, Credit, Ensemble, Machine learning*

1. INTRODUCTION

A fraud has taken place when there is an evidence of intent to mislead, cheat or steal for personal gains [1],[2],[3],[4]. However, to intentionally produce deceptive data is also a fraud.

The revelation of hidden patterns and features in data through data mining has allowed for machine learning solutions to fraud detection [5]. Machine Learning employs data mining approaches and other learning algorithms in building models of what is happening behind some data to end up in making predictions or detections. There are supervised and unsupervised learning techniques used in detecting fraudulent acts in various domains. Labelled data can be expensive and difficult to get, but this is what a supervised learning approach uses [6]. Grouping bank credit transactions into "legitimate" and "fraudulent" is a sample of labeling. Training and learning of input variables are channeled towards these target variables. Unsupervised learning uses unlabelled data, which are readily available [7]. Classification and regression are good examples of supervised learning, they easily discover duplications when some variables get tweaked, but cannot discover new situations or scenarios

Unsupervised learning examples include, clustering, outlier detection, and association. They can discover new situations or scenarios, for instance a new disease out of the listed diseases. Unsupervised learning methods can still perform well with some missing data, while supervised learning cannot operate with missing data. Therefore, machine learning is employed in modern day fraud prediction and detection. This work does a systematic literature review of fraud prediction in bank credit administration. The paper is structured as follows. Section 2 covers the theoretical framework, while the third section presents the method, followed by results in section 4; discussions in section 5; findings in section 6, and then conclusion and future works in section 7.

2. THEORETICAL FRAMEWORK

Bank credit administration all over the world has witnessed an unrepentantly high rate of fraud; this is also evident in many other sub-sectors of the economy. It is worthy of note that the traditional ways of detecting frauds in bank credit

operations today are unfit because they are inefficient and time-consuming. This is due to the sophistication involved in the 21st century methods of fraud practices. Credit fraud is one of the numerous risks that financial institutions face; it ultimately leads to credit default. This is the highest risk area for financial institutions; it is also a big hole to the treasuries of diverse countries. A host of approaches have been engaged, including statistical methods, knowledge discovery, and case-based reasoning. However, with the ever-increasing large volume of data involved, the application of data mining approaches alongside some sophisticated machine learning algorithms have opened up new ideas towards addressing the problem of credit fraud as one of the existing financial fraud.

2.1 Financial Fraud

Any unlawful act by human beings or invoked by machines that leads to a personal gain at the expense of institutions or the legal human beneficiaries, and not in an error is a financial fraud [2],[5],[3],[4]. Considering the overall effect of financial frauds, it is referred to as an economic sabotage. The examples of financial fraud are money laundering, bank credit fraud, pension fraud, co-operative society fraud, tax evasion, telecommunications fraud, credit card fraud, inflated contracts, financial reports fraud, health insurance fraud [8] automobile insurance fraud, and mortgage insurance fraud…

According to [4], people perpetrate financial fraud because of greed, gambling, debts, poor investments or because they live beyond their means or source of income. Finally, financial fraud destroy systems, deprive legal beneficiaries of loans access to qualified loans in the case of credit administration due to credit defaults, it leads to death in certain cases, for example, pensioners deprived of their entitlements due to financial frauds. Financial fraud halts the growth of economic development of nations. It is high time researchers employed technology to address the impending halt of economic growth, specifically due to credit default.

Financial fraud is increasing at a geometric rate in the society. Accounting and auditing skills have been employed for decades but can no longer withstand the current trends of fraud at this age and time. With the advent of the internet, frauds that can run down a whole country can take place in a few seconds with a few clicks of the mouse. Fraud detection must step up in the face of sophisticated methods of committing financial frauds. Machine learning is able to come to the rescue due to its sophisticated pattern recognition in data, revealing trends that give insights to what manual, semi-automated, or many automated attempts cannot reveal.

According to [9], there are many types of fraud including, credit card fraud, telecommunication fraud, computer intrusion, bankruptcy fraud, theft fraud or counterfeit fraud, and application fraud. However, based on a thorough review of the domain, this work presents the types of fraud as shown in figure 1 in the appendix [10].

2.2 Credit Fraud

In literature, there are three principal types of credit fraud, namely: Credit card fraud, credit application fraud, and bankruptcy fraud [11],[12].

2.2.1 Credit Card Fraud

This is the most predominant type of fraud experienced in credit administration. A card theft has taken place and a legitimately issued card is used by a card thief to undertake illegitimate transactions. In this scenario, the approved and registered owner of the card is unaware of his or her card's usage without approval. The fraudster suddenly engages in numerous transactions on the account of the rightful card owner without his or her knowledge, all in a considerably limited time of action. Before the legitimate card owner discovers a foul play and report to the issuer of the card or the bank, a lot of damage must have been done [13]. In literature, credit card fraud is categorized into two; offline fraud and on-line fraud [12]. The offline fraud is carried out with the use of an illegally possessed physical card at points of sale or other places of financial transactions based on cards, while on-line fraud is committed with the use of internet, phone, shopping, web, or when the person in possession of the card is not present.

Offline Credit Card Fraud: The offline fraud entails the theft of the physical card for the intention of perpetrating fraud with it in stores [12]. Much work has been done against the possibility of successfully effecting this type of a fraud, though it still exists today but it has been reduced drastically. Since the cards are part of our possessions that are used daily for diverse purposes, a loss or theft of the physical card is easily realized nowadays. The legitimate owner therefore raises an alarm to the issuer bank before any intended fraudulent transaction is carried out with that card. It is the responsibility of the bank to instantly block any reported physical card that was stolen or lost because it is already compromised. Such a physical card cannot be used any longer or until the right

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

owner has finally convinced the bank it was not compromised and the password is changed from the bank. This returns the card to a new one and certain operations to preserve the confidentiality and privacy on that card are reinforced. If a stolen or misplaced physical credit card was never reported, the policy of the banks places the responsibility on the card owner to bear the loss. This is a policy already agreed to and signed at the point of issuing the card. In some countries where the postal system is effective, banks do send freshly issued cards by post; this is perceived highly dangerous and opens the door for a theft in transit before it reaches the registered address of the card owner.

Online Credit Card Fraud: The online fraud is successfully executed based on the access to the sensitive and confidential details of the card. The unlawful access to these details is either due to a theft of the card or a careless exposure or disclosure of the details during transactions on the card by the owner; phishing and social engineering often lead to the illegal custody of these details by the fraudsters to make illegal transactions online. There is no need for a physical presence of the card to carry out a fraud using the card, for this reason it is called a virtual card theft. The antidote to this kind of a fraud remains an extreme safety consciousness, it is very difficult to prevent this type of a fraud, the fraudsters can keep the card's information for a long time before they are used [13]. It is impossible for the card owner to be aware of the theft of the credit card details until some illegitimate purchases or payments for services have been made through the card, a detection in advance is almost impossible. There are some established ways through which fraudsters steal credit card information, for example, in identity fraud as discussed below.

Identity Fraud: In an identity fraud, a fraudster uses a false identity intentionally, in order to commit fraud and hanging the crime on an innocent person or a non-existent personality [14],[15],[16]. It is common in this class of a fraud to invent a fake identity or stealing the real identity of an existing person [11],[14],[15],[16],[17].

The process of gathering the necessary information to impersonate a potential victim is cumbersome. However, fraudsters are undeterred, they can break into potential victim's houses, illegally access emails, and employees doing sensitive operations that have access to identity information are compromised in some cases. It is also common to employ malicious codes, for instance, malwares to illegally gain access to potential victims' computers online to obtain information that are confidential to their owners [14],[15],[16],[17].

The invention of a non-existing identity is difficult in the 21st century, banks and other sensitive institutions ensure the supplied information is matched to a physical person, seen, and have biometrics captured to avoid this type of a fraud.

In a situation that a fraudster has beaten the issuing bank to obtain a credit card using an invented identity belonging to a non-existent person, the bank is at a loss because the fraudster would overdraft the credit card account with the bills left unpaid [16]. If a real identity was used, the real person must pay the bills except the identity theft is proved beyond any reasonable doubt. However, the creditworthiness of the real customer is affected with reservations to be issued a credit card and also to be granted a loan later.

2.2.2 Credit Application Fraud

There is an occurrence of a credit application fraud when a fraudulent person applies for a credit card with false information or identity. A reliable profile is being built to successfully open an account and get required cards using fake documentation [11]; therefore it is closely linked to the identity fraud.

2.2.3 Bankruptcy Fraud

A situation where clients or customers use their credit cards for their expenditures beyond what they can pay is called bankruptcy fraud [11]. The credit card is an outlet for customers to take credit from their banks and the cards are used each day for various payments for goods and services. It is a routine process by banks to get across a bill to their customers in an attempt to ensure a timely payment of their credit card purchases; the bill is sent monthly to avoid any disagreement or discrepancies from both sides.

Some customers who are potential fraudsters do spend beyond their limits intentionally and apply for personal bankruptcy, this is termed a bankruptcy fraud, and the bank is obligated to pay for the losses incurred by another entity[11].

According to [18], bankruptcy fraud is increasing geometrically causing a resounding loss to the banks who are the creditors and issuers of credit cards. Also, an evaluation of credit card applications for the verification of credit worthiness was proposed by the authors. The evaluation is expected to reveal it if a customer is likely to go bankrupt in the near future. It is worthy of note that despite the evaluation, the customers adjudged to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

be credit worthy can still go bankrupt at a later time. Therefore, when a customer is provided with a credit card account based on being considered credit worthy, there is a need for monitoring if the bank would not end up losing money as a bankruptcy fraud is not impossible.

When credit card bills payments are not consistently paid, it is an indication to a potential bankruptcy fraud [19]. It is high time the banks took drastic measures to have their losses due to bankruptcy fraud significantly reduced. The allowable credit card limit could be reduced in order to minimize their loss in case of a bankruptcy. Also, the banks need to temper justice with mercy because some customers genuinely had difficulty in paying their bills but a limit on their cards can make them close their accounts. This is not good for the banks and the scenario must be avoided.

2.3 Data Mining

Data mining is the computational process commonly employed in the analysis of huge datasets, for the discovery of important trends, and extraction of paramount knowledge for the prediction of hidden knowledge. Many subfields of computer science are involved in its functional concept. Artificial Intelligence, Statistics, Mathematics, Machine Learning, and Database Systems. Pre-processing operations are important prior to the execution of data mining algorithms. There is also a post-processing stage employed for the visualization of the analysis results (identified patterns or retrieved knowledge) with basic intuition and ease of communication.

Algorithms in this domain are of two categories, namely: Prediction and knowledge discovery. The sub-categories of note are: Classification and regression, clustering, association rule mining, and outlier or anomaly detection. Some evolving data analytics are the spatial and graph data mining coined out of the constituents of data mining approaches. Datasets of huge instances and variables are the best for data mining approaches and delivers enhanced accuracy. In circumstances of conventional statistical approaches failure, better insights are revealed in high-dimensional datasets.

A thorough analysis and formalization of desired objectives are critical in an effective data mining solution. This guides the choice of a learning algorithm to use. To see clearly unclear groups in data or discover associations existing in important data variables (knowledge discovery), the choice of clustering or association algorithms is inevitable. However, if the objective is prediction or classifying variables into specific categories, classification or regression approaches are to be employed.

2.4 Machine Learning

Machine Learning employs data mining techniques and other learning algorithms to build models of what is happening behind some data to make predictions or detections [20].

With basic human services being rendered daily, a large range of data is generated with basic characteristics of volume, variety, and volatility. According to [21], the existing dataset have numerous untapped potentials, challenging traditional ways of solving problems. With the real-time operations that are evident in the information age, the need for pattern recognition, information extraction, predictions, and detections cannot be over-emphasized. Machine learning and data mining tools are being employed to solve fraud prediction and detection. Machine learning is basically categorized into supervised learning and unsupervised learning.

2.4.1 Supervised Learning

This is a very common learning method; the model gets trained with the use of pre-defined class labels. In a financial fraud detection context, the class labels could simply be legitimate or fraudulent transactions.

The training dataset is employed in building the model, thereafter; new transactions can be compared with the already trained model for a prediction of the class it belongs to. A transaction is classified legitimate when it has the same pattern with the trained legitimate behaviour, else, it is classified illegitimate. One of the merits of supervised learning is that the classes are comprehensible to human beings, and therefore employed for pattern classification.

However, it is difficult to gather class labels; also, with a bulky data input, it gets expensive to label all. It is worthy of note that transactions must be correctly identified to reduce false positives and true negatives. The models in supervised learning cannot detect new types of fraud apart from those trained to be included as target class. For example, in diseases prediction, any disease not included as one of the target diseases is never detected. An unsupervised learning isolates such as a new disease, though not one of the expected diseases, but based on a different trend discovered, it will be set aside. However, supervised learning discovers fraudulent duplicates in fraud detection which unsupervised learning cannot do. Supervised

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

learning problems are either regression or classification problems as discussed below.

Regression versus classification problems: According to [22], variables can be characterized as either quantitative or qualitative (also known as categorical). Quantitative variables take on numerical values; for instance, the age of a person, height, or salary; a car's selling price, and the cost of a drink. However, qualitative variables take on values in one of y classes, or groups. Examples of qualitative variables include the complexion of a person (dark or light), the type of account operated in a bank (A = savings, B = current, or C = special), confirming if a man is physically challenged or not (yes or no), or a fever diagnosis (Malaria, typhoid, free).

The problems that have a quantitative response are called regression problems, and the problems that involve a qualitative response are called classification problems. However, to distinguish them is quite easy; the least squares linear regression is meant for a quantitative response, while logistic regression is employed for a qualitative (two-class, or binary) response; therefore, it is utilized as a classification approach but since it does the estimation of class probabilities, it can be classified as a regression method too. There are some statistical approaches, for example, K-nearest neighbors (KNN) and boosting, can be used in both of quantitative and qualitative responses [22].

Statistical learning methods are commonly selected based on whether the response is quantitative or qualitative; thereby, using linear regression when quantitative and logistic regression when qualitative. However, the quantitativeness or qualitativeness of the predictors is not paramount. Most of the existing statistical learning approaches are suitable for use irrespective of the predictor variable type, resting on the criterion that qualitative predictors are properly coded prior to the performance of the analysis [22].

Selection of classification methods: In the fraud prediction domain, classification methods are selected based on the following criteria: Ability to handle huge datasets of high dimensionality with very good efficiency and with desired accuracies; ability to provide easily understood results for business experts; performance metrics are based on highest classification accuracy (researchers), generation of understandable and practical classification rules (industry practitioners' concern). Classification techniques have been employed in many domains like, facial recognition, age estimation, features extraction, stock prediction, fraud detection, malware detection and many others [23],[24],[25],[26].

Classification machine learning algorithms: Classification is a supervised machine learning method where datasets are labelled. The goal is to have data prediction in a predefined group. Examples of classification algorithms are the Neural Networks, Genetic Algorithm, Support Vector Machine, Bayesian Networks, and Decision Trees; and they are discussed below.

Naive Bayes: Bayesian Classifiers are statistical classifiers for the prediction of class membership probability that a given sample belongs to a particular class. This is a simple method, elegant, and robust. It is a classification algorithm that has been in existence long ago and despite its simplicity, it is an efficient machine learning approach. It has a wide coverage of applications, for example, in spam filtering, text classification, image processing [27]. To enhance its flexibility, it has been modified numerous times in statistics, machine learning, and pattern recognition domains. Bayesian Networks are graphical models that show

$$P(x \mid K) = \frac{P(K \mid x)P(x)}{P(K)}$$

relationships between the subset of attributes. Every Bayesian Learning Algorithms has its root in the Baye's Rule.

The Baye's theorem

P(x) = the initial probability of hypothesis x

P(K) = the initial probability of training data K

P(x|K) = probability of x with K provided

P(K|x) = probability of K with x provided

Naive Bayes algorithm. The conditional independence of the attributes of the instances is needed to use Naive Bayesian Classifiers.

X be a set of instances $X_1 = (a_1, a_2, \ldots, a_n)$

V be a set of classifications v_j

The Naive Bayes assumption is as follows:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and it follows that the algorithm is

$$v = \max_{vj \in V} P(v_j \mid a_1, a_2 .... a_n)$$

$$= \max_{vj \in V} \frac{P(a_1, a_2 .... a_n \mid v_j) P(v_j)}{P(a_1, a_2 .... a_n)}$$

$$= \max_{vj \in V} P(a_1, a_2 .... a_n \mid v_j) P(v_j)$$

$$P(a_1, a_2 .... a_n \mid v_j) = \prod_i P(a_i \mid v_j)$$

implemented thus:

Naive_Bayes_Learn (examples)
for each target value v_j
estimate $P(v_j)$
for each attribute value a_i of each attribute a
estimate P(ai | vj)
Classify_New_Instance (x)

The training takes a short computational time and the model is easily constructed; it is suitable for large dataset and the iteration parameter estimation is less complicated; the represented knowledge is easily interpreted; it is not specific to an application in its strength but it is robust and does well across board.

Support vector machine (SVM): The SVM was developed by [28], based on the structural risk management theory [29]. It uses decision planes to define decision boundaries, separating between a set of objects with diverse class memberships. The SVM creates a hyperplane by using a linear model to implement non-linear class boundaries through some non-linear mapping input vectors into high dimensional feature space [30].

The SVM has been employed in many detection and prediction works, for example, telecommunications, pattern recognition, system intrusion detection, age estimation, and facial recognition [23],[24],[25],[26],[31][32]. Figure 2 (appendix) is a diagrammatic representation of a sample support vector machine implementation [30].

Support Vector Machine (SVM) is a classification and regression prediction tool that employs machine learning theory in the maximization of its predictive accuracy as it automatically avoids overfitting to the data. Support Vector machines are systems that use hypothesis space of a linear functions in a high dimensional feature space, trained with a learning algorithm from optimization theory that implements a learning bias derived from statistical learning theory. SVM came to limelight when it outperformed the well-known sophisticated neural networks based on elaborate features in a handwriting recognition problem, using pixel maps as input. It is notably applied in hand writing analysis, face analysis, and more interestingly for pattern classification and regression based applications.

Its better empirical results have given it prominence, the SVM uses Structural Risk Minimization (SRM) principle, and this has proved superiority over the conventional Empirical Risk Minimization (ERM) principle that is used by conventional neural networks. It is worthy of note that SRM operates by a minimization of an upper bound on the expected risk, and in the case of ERM, the training data error is being minimized by it. This difference affords the SVM with the capability of generalization, and that is the essence of statistical learning. SVMs were initially meant for classification problems but currently, an extension of it makes it suitable of solving regression problems too.

The statistical learning theory makes available a framework that studies the problem of gaining knowledge-gaining, predictions-making, decisions-making, based on the available dataset. The choice of the hyper plane space is done in way that the target space underlying function is closely represented.

In statistical learning theory the problem of supervised learning is formulated as follows. Given a set of training data $\{(\mathbf{x}_1,y_1)... (\mathbf{x}_l,y_l)\}$ in $R^n \times R$ sampled according to unknown probability distribution $P(\mathbf{x},y)$, and a loss function $V(y,f(\mathbf{x}))$ that measures the error, for a given $\mathbf{x}$, $f(\mathbf{x})$ is "predicted" instead of the actual value y. The problem consists in finding a function f that minimizes the expectation of the error on new data that is, finding a function f that minimizes the expected error: $\int V(y, f(\mathbf{x}))\, P(\mathbf{x}, y)\, d\mathbf{x}\, dy$

In statistical modeling, a model is chosen from the hypothesis space, which is closest (with respect to some error measure) to the underlying function in the target space.

Decision tree (DT): The decision tree classifies data into discrete ones using tree structure algorithms [33]. It highlights the structural information contained in the data. It builds a decision tree from a set of class labelled training samples during the machine learning process [34]. Each internal node in a decision tree is a test on attribute (feature); each branch is an outcome of the test; and each leaf node is the class label.

In its classification exercise, it identifies the class label of an unknown sample, tracing path from root to the leaf node, which holds the class label for that sample [34],[35].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Decision tree algorithm

1. Provide the root node N
2. In case every sample belongs to an identical class C
   then return the node N as leaf node with the class labeled C
3. In the absence of any feature, return N as leaf node with the most common class of samples
4. Apply the feature selection measure to select the best feature
5. Label node N with the feature found in step 4, called test feature
6. For each value V_i of test feature
   a. Partition the samples and grow subtree for each value V_i of test feature.
   b. Let a_i be the set of tuples for which test feature = V_i
   c. If a_i is empty then attach a leaf node with the most common class in samples
7. Else attach the node returned by Generate_decision_tree (a_i, attribute_list-test_attribute).

For example, to classify a bank loan application for a customer, the decision tree could be as shown in figure 3 (appendix).

The advantages of using decision trees: The simplicity and speed of decision trees is second to none; there is no requirement for a domain knowledge or parameter setting; it comfortably handles high dimensional data; the way it is represented allows for enhanced comprehensibility; it has a fantastic accuracy though this is dependent on the data in use; it supports incremental learning, and they are unvaried, since they are used based on a single feature at each interval node. It is also worthy of note that decision trees work fine on both classification and regression problems; they can handle missing values; the trees are plotted graphically, and can be easily interpreted; trees can be easily explained to people [36],[37],[38]. Other approaches include Artificial Neural Networks, and K-Nearest neighbour. Table 1(appendix) is a comparison of common classification techniques[39] - [46].

2.4.2 Semi-supervised learning

As it was discussed earlier, supervised learning needs every training sample for the labeling of their classes; but unsupervised learning requires no labeled samples for its required operations. Semi-supervised learning is a bridge between the two main classes of learning as a small number of labelled samples are required and a large number of unlabelled samples [47]. In the domain of fraud detection and credit card fraud detection specifically, semi-supervised learning techniques may involve labels for some of the legitimate transactions only. Therefore, it reduces the effort supervisors require in the classification of training data [47]. The artificial immune system is a good example of this category.

Artificial immune system (AIS): The Artificial Immune System (AIS) is an artificial intelligence-based approach that mimics the operations or functionality of the human immune system [9],[10],[48]. Categorization of all the body cells into self or non-self cells forms the basic function of the human immune system [9],[10][48],[49]. The self (S) cells represent every pattern in a finite space that is legitimate and non-self (N) is a representation of illegitimate cells [9],[50],[51]. The non-self cells are then thoroughly examined to conclude on a suitable defence [10],[51].

The AIS consists of artificial lymphocytes (ALCs) that are able to classify any pattern as self or non-self by detecting only non-self patterns. AIS detection engines implements AIS based algorithms which can classify input data as normal or fraudulent [48]. For a future reference, the defensive mechanism that has been used to protect the body from a non-self cell N previously is kept. If a non –self cell similar to N invades the body later, the preserved defensive mechanism comes to a rescue. Therefore the immune system is able to protect the body from non-self cells by applying an evolutionary learning mechanism [49]. It is interesting to note that our immune system can also spot new types of non-self cells which are unknown and not seen before [48].

An AIS is a mimicry of the human immune system. In the fraud detection domain, an AIS discovers illegitimate transactions because they are perceived as the non-self cells [48]. An exhaustive labelled training is not required to achieve this task. However, a limited volume of labeled samples are presented corresponding to legitimate transactions and a huge volume of unlabelled samples corresponding to either legitimate or illegitimate transactions. By virtue of this, the AIS is a semi-supervised learning approach that identifies both previously seen fraudulent patterns, and others that have not been seen before.

2.4.3 Unsupervised learning

This category has no class labels. It finds instances that show unusual behavior. These techniques endeavour the discovery of both old and new fraud types. There is no restriction to the fraud patterns that already have predefined class labels like

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

supervised learning techniques do. It detects anything that does not abide by the normal behavior; this is due to its directionless nature, it finds patterns that are of no prior notice or recognition. These are basically association rules, clustering, and outlier detection.

Outlier detection (OD): This refers to a situation where in the course of an observation, a particular point or group of observed facts have deviated from common scenarios or points to perceive it was a product of a different mechanism. Outlier detection is an unsupervised learning approach that discovers strange patterns in data [52]. A detection of outliers is easily done even without knowledge of the dataset distribution or a requirement for training samples that are labeled [53].

A careful choice of similarity metric is of utmost significance in the study of the complexity of outlier detection [54]. This does a calculation of the similarity amongst diverse data. The type of metrics used determines the outcome, therefore; the choice of a right metric is critical and may be a complex step [10],[54]. In a fraud detection work, a fraudulent transaction is an outlier with a dissimilar behavior compared to the legitimate ones which are commonly in the majority; therefore the outlier is easily identified.

Peer group analysis (PGA): This is an unsupervised learning approach that does a monitoring of behavior over a period of time [55]. In the scenario of a fraud detection in credit administration, the PGA takes note of all creditors account **X** that behaves like a target account **Y** at a past time $\mathbf{t_{past}}$ [54]. The accounts X are the "peer group" of Y. The target account Y is being suspected of a fraud if and only if at the current time $\mathbf{t_{current}}$ it behaves differently from its peer group X. This approach is able to avoid flagging a transaction as fraudulent if its peer group undergoes the trend it undergoes at a time. For instance, when teachers' salaries are not paid, all teachers might not fulfill their expected repayment pattern. When a client is compared with others in its group, a reason for the untoward pattern might be discovered and unnecessary false positives are avoided.

Hidden Markov model: According to [10],[56] "hidden Markov model is a double embedded stochastic process with two hierarchy level." In a comparison with the conventional Markov model, hidden Markov model is better in terms of expressiveness and it is more advanced in its representation of stochastic processes. This approach is popular in some strategic domains of research including speech recognition, computer vision, and pattern recognition. The work of [56] also employed the hidden markov model in the domain of fraud detection; specifically in credit card fraud detection.

2.5 FEASIBLE CHALLENGES ASSOCIATED WITH THE PREDICTION TECHNIQUES

Noise: Data do witness the presence of unwanted figures or errors, for example, incorrect date, wrong date of birth or age; when some values are missing, these are also noise, and they collectively lead to a wrong model construction and ultimately inaccurate predictions [10],[57]. The removal of noise from data to be used for machine learning and other tasks is a critical step, and this is referred to as cleansing, this could be tasking in some cases, but it depends on the dataset in consideration.

Labelled training samples: The process of seeking and finally getting a reliable training data samples and effectively group to the right class labels for model construction can be a tough task in the research procedure. Supervised learning approaches only work with labeled data, and more often than not, this is not readily available or there is a need to go an extra mile to finally arrive at this for an effective training, testing, and validation [47].

Overlapping data: This scenario occurs when there is a misrepresentation of the reality; when an illegal transaction appears like a legitimate one or when a legal transaction looks very similar to a fraudulent one. This is a height of confusion that can make the process of model construction complicated and faulty.

Parameters choosing: Each of the data mining approaches need many parameters, this includes the thresholds to be set earlier by the user. The variation in the choice of parameters affords a unique diversity in the performance of the constructed models, and this leads to an increment in the complexity of the constructed model [58].

Feature selection: The process of choosing the features also referred to as attributes or columns of the available dataset in the construction of the detection model could be a daunting task on several occasions. The features selected determine to a large extent the predictions being made by the machine learning approach, this is critical since they are used for critical decision making and the judgement of the machine learning approach is trusted.

Overfitting: Despite an effective pre-processing of training dataset that includes data cleansing, there are still some existing errors or random values referred to as small fluctuations in that dataset [59]. Overfitting is the aftermath of a situation when the

machine learning algorithm employed in the model construction attempts to learn as many as available information from the training dataset without an exemption of the small fluctuations that deviate from the real situation. This turns out to yield a very complex model and poor predictive accuracy [10].

2.6 Hybrid learning

The hybrid method employs majorly unlabelled data with a blend of some labelled input data. The fact that some labelled data is included boosts how efficient the supervised learning becomes. In order to make predictions, the learning of the model includes the structure and the organization of data. The work in [60] features a 3-step procedure for detection of fraud in the insurance sector. It employed an unsupervised learning approach, specifically clustering on claimed insurance benefits; this was followed by a modelling of a variety of labelled clusters. In order to bring in a supervised learning, a classification tree algorithm was employed as a supervised learning; this led to the discovery of rules for the allocation of each record of clusters. The work provided very effective rules to identify fraud behaviours of the future.

The aim of hybrid learning is to afford a combination of labelled and unlabelled data, such that every weakness in any of such data is complemented; thereby changing the learning environment and formulating algorithms to attain efficient fraud detection. This is a great paradigm in machine learning and data mining for effectively using unlabelled data for improvising supervised learning that should use labelled data which are not very much available and also costly. Graph-based methods and semi supervised support vector machines are some examples.

The difficulty in obtaining labelled data and the availability of unlabelled data cannot be over-emphasized, though the unlabelled data are inefficient in the detection of fraud. The hybrid approach is a long- awaited solution to reduce human effort and enhance accuracy [5].

2.7 Ensemble Learning

This is a machine learning paradigm that is based on the training of multiple learners to solve a particular problem. For the purpose of comparison, it is worthy of note that machine learning approaches do learn one hypothesis from training data, while ensemble approaches do construct a set of hypotheses and do a combination of those hypotheses for use.

An ensemble is a combination of many learners referred to as base learners. A collection of various strengths in each base learner and finally working on their shortcomings results in an ensemble that is more efficient, effective, and robust than each of the base learners who in each of their classes are worthy problem solvers on their own, thereby a more reliable solution provider is delivered.

The base learners can be decision tree, neural network, K-Nearest neighbor or any other machine learning algorithm. Most ensemble methods use a single base learning algorithm to produce homogeneous base learners, but there are also some methods which use multiple learning algorithms to produce heterogeneous learners. For the last category, the base learning algorithms are referred to as individual learners or component learners by some people instead of the popular base learners.

The cogent idea of deploying multiple models has been on for a long time. However, ensemble learning earlier researches anchor on two works; [61] leading to a revelation that predictions from a combination of a set of classifiers are of a better accuracy than predictions from any perceived best single classifier. The other is [62] which provided the evidence that weak learners can be boosted to strong learners,which gave birth to Boosting, which today is one of the most employed and reliable ensemble approaches.

Some domains where ensemble learning has been used include: Optical character recognition, text categorization, face recognition, computer-aided medical diagnosis, gene expression analysis. Wherever machine learning techniques can be used, ensemble learning can be employed for better results. Improving the comprehensibility of ensembles is is a channel for future works as it is currently understudied; however, it deserves the attention of researchers [63].

The employment of different base learner generation processes or different combination schemes leads to different ensemble methods. Boosting, Bagging, and Stacking are the three representative effective and foundational ensemble methods [62],[64],[65],[66] in literature.

The weighting strategy of AdaBoost is equivalent to resampling the data space [67], which are applicable to most classification systems without changing their learning methods. Besides, it could eliminate the extra learning cost for exploring the optimal class distribution and representative samples [68]. Moreover, compared with the method of eliminating samples from data set, it reduces the information loss, overfitting risk

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and bias error of a certain classification learning method [69].

2.8 Related Work

There are many related works done in fraud detection, spanning from unsupervised learning, supervised learning, and hybrid approaches, being applied in numerous domains of human endeavor. The prominence of fraud detection researches with machine learning approach solutions is evident in the health, automobile, crop, and mortgage insurance [2],[5],[70]; telecommunications [26]; credit cards [9]; financial reports [71]; and money laundering [72],[73].

In [74], financial frauds were categorised into bank fraud, corporate fraud, and insurance fraud. This work has categorized credit fraud as a bank fraud. Further categorizations are as presented in Figure 4 (appendix) [74].

Fraud categories and detection algorithms: In literature, many approaches have been used in various domains to detect frauds including credit card frauds, insurance fraud, and financial statement frauds. Also, a host of machine learning approaches have been employed, for example artificial immune system, text mining, genetic algorithm, fuzzy logic, and others as revealed in Figure 5 in the appendix [74]

Fraud detection is a rich domain of research in the academia and the industry. The strength of techniques like decision trees, neural networks, and Bayesian networks were studied in [75] and a comparison of those techniques was done. Also, a summary of the available classification methods for financial fraud detection was explored in [76], and [77].

In [78], a credit card fraud detection model was developed based on frequent itemset mining. The work also employed a matching algorithm to discover the closeness of an incoming transaction to either legitimate or fraudulent for a decision to be made. A highly imbalance and anonymous credit card transaction datasets were used and the proposed model evaluation revealed a high fraud detection rate, and balanced classification rate.

The proposal for building a classification model in the detection of credit loan fraud based on individual level utility was evolved in [79]. The work confirmed the geometric increase in bank credit services and the corresponding fraud. There is a need for intelligent detection of bank credit fraud. The focus on individual level utility by this model singles it out from other works. This work carried out its preprocessing and feature selection, and thereafter effected its utility-sensitive classification model based on decision tree, Bayesian networks, and bagging for the prediction of the probability of each credit client being fraudulent. The data used covered a period of six months from a financial institution. However, the duration could be increased for a better result despite the claimed satisfied performance of this work.

The work in [80] used the random forest to detect credit card fraud making use of historical transaction data using legitimate and illegitimate transactions to obtain fraudulent and legal behavior features using machine learning. This paper specifically utilized two types of random forests (random tree-based and classification and regression trees CART-based random forest) to train the behavior features of legal and fraudulent transactions using e-commerce company data in China. The work compared the random forests that are different in their base classifiers with performance analysis for detecting credit fraud.

In [81], a consumer loan payment default predictive model was developed with a study of consumer behaviour in terms of loans payment default using logistic regression and discriminant analysis. Also, [82] did a review of prediction system for bank loan credibility using the random forest algorithm. However, all these can be made through an ensemble approach in order to discover undefined fraud patterns in training or testing that can be revealed through an unsupervised learning.

The work of [83] was on the prediction of microfinance bank credit default and the factors leading to such prediction. It employed a logistic regression approach leading to favourable results. In [84], a collection of regression and classification approaches of stepwise regression, logistic regression, support vector machine, decision tree were employed to forecast possible areas of fraud in financial statements.

The work of [85] employed ensemble tree learning methods and Genetic Algorithm to discover financial fraud. This work was specific to fraud in credit cards using the UCI (University of California, Irvine) machine learning repository using the German credit card dataset and Australian credit card dataset. The Adaptive Boosting (AdaBoost) was employed to enhance the decision tree and implemented in WEKA [86]. It is evident that the AdaBoost can be applied to other classification learning algorithms [87].

According to [88], in the previous fraud detection works, the crucial characteristic of fraud data that it is imbalance has been ignored. It is

imbalance because the number of valid records is largely smaller than the number of illegal fraud records. To enhance the prediction accuracy of fraud detection techniques, many combination of individual approaches to boost the effectiveness of those approaches have been employed. The work submits that the ensemble approach is the best, working with imbalance data, and proposed an approach that combines the bagging and boosting techniques together, in which the bagging technique can reduce the variance for the classification model through resampling the original data set, while boosting technique can reduce the bias of the model.

3. RESEARCH MODEL

This systematic literature review was carried out based on [89] as a model, and fundamentals towards a smooth conduct of study leveraged on [90].

3.1. Research Question

This study seeks to answer the question below:
1) RQ: What is the trend of research and the level of researchers' interest for financial fraud prediction in credit administration, with a look out for the least and most researched issues? In the pursuit of a cogent answer in this direction, a review of current works in literature was carried out.

3.2 Inclusion and Exclusion Criteria for Considering Studies for this Review

From January 2018 to September 2018, the process of gathering relevant information based on diverse literature was in the front burner. However, the work was finally restricted to the Information Technology and Computer Science domains, this is in tandem with the work of [91],[92]. The detailed inclusion and exclusion criteria applied to this review are illustrated in Table 2 (appendix).

3.3 Search Strategies for Choosing Relevant Publications

Six cogent steps were taken in the process of searching for literature as detailed in the description column of table 3. Google Scholar and Researchgate, IEEEXplore, ScienceDirect, Scopus, ACM Digital Library, and SpringerLink played a prominent role in this regard. Search terms were grouped into three categories of interest: Bank credit fraud prediction, employed machine learning techniques, and financial fraud. Each category of search terms was used as single items or in combination by using the Boolean operators "AND" and "OR". Table 3 in the appendix is the systematic literature and information search strategy

A combination of keywords was employed, testing for synonyms used in the literature and to cover a variety of publications on fraud prediction in credit administration. The search terms below were employed. The following combinations of search terms were applied:
Fraud prediction OR credit fraud reviews OR bank credit fraud prediction OR financial fraud OR bank credit fraud survey OR loan fraud detection literature review OR machine learning fraud prediction OR fraud detection using hybrid learning OR ensemble learning fraud OR credit default fraud detection OR bank credit fraud review AND Information Technology OR Computer Science**.**

4. Results

The search of this work had an initial selection of n = 308 publications; out of these, n = 251 were chosen from databases (search steps 1 and 2, Table 3). Furthermore, n = 57 were selected through open search on websites and establishing contacts with individuals (search steps 3–5, Table 3). In step 1, we took off n = 120 articles based on the consideration of the language of communication, title and duplicates had to be deleted. The remaining n = 188 publications were then reviewed, and a further n = 143 got expunged for not meeting the inclusion criteria as indicated in Table 2. In the final step of selection, the ensuing doubts about the work was resolved through a comprehensive discussion including all authors, this led to the inclusion of an additional study from the references list in one of the publications. Finally, 46 studies were selected to have fulfilled all the laid down inclusion criteria and thereby included in this review.

The highest number of papers accruing to 6.4% was published in each of 2012 and 2013, followed by 5.6% in the years 2008 and 2015. The years 2014 and 2016 came third with 4.8% each of the analyzed papers. The year 2017 featured 4.0% coming fourth, followed by 3.2% in 2011, then 2.4% each in 2002, 2007, 2009, 2010. Other years in consideration contributed 0.8% except for the year 2008 with 1.6%. The papers analyzed are 35% from conferences, 58% journal articles, and 7% from workshops, technical papers, and surveys, all in fraud prediction in credit administration, either covering the techniques of prediction, surveys, reviews, machine learning, hybrid or ensemble learning.

4.1 Search String

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Right from the beginning, the scope of the research was clear and were based on the concept, techniques for prediction, gaps in research, and suggestions. Research questions and keywords were identified based on these prior definitions, therefore standard and referred databases were consulted. We combined keywords to test for synonymns in title to ensure a robust coverage of relevant publications on fraud prediction in credit administration. The different search string combinations are as listed in section 3.3 earlier.

4.2 Purpose of Intervention

All studies included in this review focused on bank credit fraud prediction, employed machine learning techniques, and financial fraud. It is worthy of note that to the best of our knowledge, no systematic literature review for bank credit fraud is existing but rather in credit card fraud or health insurance fraud. The work of [76],[88],[93] [94] [95].
are on financial fraud detection generally using specific approaches but not reviews. Financial statement fraud detection using hybrid approaches.

In [71],[75], and [84]; hybrid approaches were employed to detect financial statement fraud but none is a systematic literature review in that domain to give directions of research. Health Insurance fraud prediction has received attention in many dimensions based on diverse approaches, [2],[8],[24],[27]. Furthermore, [57] employed a hybrid approach; and a survey of hybrid approaches in [5] [94]; while [70] is a survey on health insurance fraud. Review of credit card fraud detection techniques was done in [9]; [11]; [20]

Financial statement fraud detection using hybrid approach was featured in [71],[75]; [84]. Machine learning algorithms are widely employed in fraud prediction as revealed in a review of ML algorithms by [40]; and a ML SLR in [21].

4.4 Risk of Bias and Challenges

To ensure an unbiased categorization after the searches, the inclusion or exclusion criteria were applied to aid decision making, it was ensured that every selected paper was scrutinized by each of the collaborating researchers for this work. However, the strategic choice of search strings determine the papers retrieved [96], and a variation in the strings used for this work could have yielded different relevant publications from what is obtainable here [94]. Furthermore, our systematic review could still be biased despite efforts to avoid bias, because the databases that we consulted, indexed more of the renowned conferences and journals on the subject of fraud prediction in credit administration; hence, the views of low class publications are ignored. Furthermore, a conduct of further searches in non-English sources can afford a reduction in the possible bias in the study.

5. Discussion

From the analysis, it was observed that there is a waveof interest in bank credit fraud analysis from 2008 to date. The amount of papers published in the domain from 2003 to 2007 was garnered in a single year of 2008, having 7 publications for the analysis. Also, there was a consistent increase in the number of publications from 2009, showing more attention in fraud prediction using machine learning in the academia. The years 2012 and 2013 witnessed the peak having 8 publications each. The latest publications for 2018 might not be completely available for analysis; hence the drop in the number of publications accessed. See Table 4 and figure 6 (appendix). Percentage of papers analyzed from journals was 58%; that of conferences was 35% while that of workshop/technical/symposium was 7% as depicted in figure 6. The views of low class publications were ignored for this study since robust and popular databases were explored. Also, papers written in other languages than English were left out. The knowledge presented here do not represent the two classes mentioned which could have enriched the presented analysis.

6. FINDINGS OF THE STUDY

The findings of this work based on the research questions explored are as follow:
RQ - *What is the trend of research interests so far in financial fraud in credit administration, in terms of the least and most researched issues?*
We discovered that existing literature have covered fraud, financial fraud, and mostly credit card fraud prediction with machine learning approaches but financial fraud in bank credit default is yet to receive attention despite the fact that this takes a toll on banks and the illegal defaults affect nations too.

7. CONCLUSION AND FUTURE WORK

In this paper, we have carried out a systematic literature review of fraud prediction in bank credit administration, in order to understand the trend of research interests so far in fraud prediction in the context of credit administration based on the least and most researched issues.

The articles surveyed in this work have used machine learning techniques to predict fraud with specific interest in bank credit administration;

several approaches were employed; ranging from unsupervised, supervised, hybrid and ensemble techniques. Machine learning algorithms, performance, and accuracy measures are of importance in the review. The survey reveals that fraud prediction accuracy is not only based on the algorithm put to use, but a function of the context of the work, data pre-processing, how the techniques are combined, strength of base learners, and a host of other factors. This paper would guide future researchers in their choice of machine learning fraud prediction techniques to use and a pointer to possible improvements on some of the existing techniques.

ACKNOWLEDGMENT
The Covenant University Centre for Research and Innovation Development (CUCRID) gave a full support to this research work.

REFRENCES:

[1] Oloidi, G.A., and Ajinaja, O. T. (2014). Bank frauds and forgeries in Nigeria: A study of the causes, types, detection and prevention. *IOSR Journal of Economics and Finance,* **4(**2): 41-50.

[2] Rawte, V., and Anuradha, G., (2015).Fraud detection in health insurance using data mining techniques. *International Conference on Communication, Information & Computing Technology (ICCICT),* pp. 1-5, Mumbai.

[3] Naik, J., and Laximinarayana, J.A. (2017). Designing hybrid model for fraud detection in insurance. *IOSR Journal of Computer Engineering*, **1**: 24-30.

[1] Author No.1, Author No 2 Onward, "Paper Title Here", *Proceedings of xxx Conference or Journal (ABCD)*, Institution name (Country), February 21-23, year, pp. 626-632.

[2] B.N. Singh, Bhim Singh, Ambrish Chandra, and Kamal Al-Haddad, "Digital Implementation of an Advanced Static VAR Compensator for Voltage Profile Improvement, Power Factor Correction and Balancing of Unbalanced Reactive Loads", *Electric Power Energy Research*, Vol. 54, No. 2, 2000, pp. 101-111**.**

[3] Naik, J., and Laximinarayana, J.A. (2017). Designing hybrid model for fraud detection in insurance. *IOSR Journal of Computer Engineering*, **1**: 24-30.

[4] Akomolafe, J. A., Eluyela, Damilola F.,Ilogho, S.O, Egharevba, J. W., and Aina, O. (2017). Financial crime in Nigeria public sector: a study of lagos state ministries. *International Journal of Innovative Research in Social Sciences & Strategic Management Techniques*, **4** (1):13-21.

[5] Bagul, P.D., Bojewar, S., and Sanghavi, A. (2016). Survey on hybrid approach for fraud detection in health insurance. *International Journal of Innovative Research in Computer and Communication Engineering,* **4**(4): 6918-*6922.*

[6] Hetal, B., and Amit, G. (2012). A comparative study of training algorithms for supervised machine learning. *International Journal of Soft Computing and Engineering, (IJSCE)*, **2(**4):74-81.

[7] Brockett, P., Derrig, R., Golden, L., Levine, A. and Alpert, M. (2002). Fraud classification using principal component analysis of RIDITs, *Journal of Risk and Insurance,* **69**(3): 341-371.

[8] Kose, I., Gokturk, M., and Kilic, K. (2015). An interactive machine learning-based electronic fraud and abuse detection system in healthcare insurance, *Applied Soft Computing*, **36**:283–299.

[9] Tripathi, K.K. and Pavaskar, M.A. (2012). Survey on credit card fraud detection methods, *International Journal of Emerging Technology and Advanced Engineering,* **2(**11): 721-726.

[10] Potamitis Giannis (2013). Design and Implementation of a Fraud Detection Expert System using Ontology-Based Techniques, unpublished dissertation, university of Manchester.

[11] Delamaire L., Abdou, H., and Pointon, J. (2009).Credit card fraud and detection techniques: A review. *Banks and Bank Systems*, **4(**2): 57-68.

[12] Laleh, N. and Azgomi, A. M. (2009).A Taxonomy of Frauds and Fraud Detection Techniques, *ICISTM,* **(31)**. pp. 256-267.

[13] Aleskerov, E., Fieisleben, B. and Bharat, R. (1997). CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection, *Department of Electrical Engineering and Computer Science, University of Siegen,* pp. 220-226.

[14] Hoar, S. B. (2001). "Identity Theft: The Crime of the New Millennium," *Or. L.,* pp. 1423-1448.

[15] Koops, B.J. and Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime, *Datenschutz und Datensicherheit-DuD,* vol. 30, no. 9, pp. 553-556.

[16] Actionfraud (2013).“Identity fraud and identity theft,” Action Fraud, [Online]. Available: www.actionfraud.police.uk/fraud_protection/identity_fraud. [Accessed 22 June 2013].

[17] C. Phua, R. Gayler, V. Lee and K. Smith-Miles, “On the communal analysis suspicion scoring for identity crime in streaming credit applications,” *European Journal of Operational Research,* vol. 195, pp. 595-612, 2009.

[18] Xiong, T., Wang, S., Mayers, A. and Monga, E. (2013). “Personal bankruptcy prediction by mining credit card data,” *Expert Systems with Applications,* pp. 665-676.

[19] Whittaker, J., Whitehead C., and Somers, M. (2005). “The neglog transformation and quantile regression for the analysis of a large credit scoring database,” *Royal Statistical Society,* vol. 54, no. 5, pp. 863-878.

[20] Chaudhary, K., Yadav,J., and Mallick, B. (2012). A review of fraud detection techniques: Credit card. *International Journal of Computer Applications,* **45(**1):39-44.

[21] Bellinger, C., Mohomed, J., Zaïane, O., and Osornio-Vargas A. (2017). A systematic review of data mining and machine learning for air pollution epidemiology. *BMC Public Health.* **17**(1):907.DOI:10.1186/s12889-017-4914-3.

[22] James, G., Witten, D., Hastie, T., Tibshirani, R. (2013). An Introduction to Statistical Learning with applications in R, springer, New York, ISBN 978-1-4614-7138-7 (eBook) DOI 10.1007/978-1-4614-7138-7

[23] Guo, G., Fu, Y., Dyer, C.R., and Huang, T.S. (2008). Image-based human age estimation by manifold learning and locally adjusted robust regression, *Transactions on Image Processing, IEEE*, **17(**7): 1178-1188.

[24] Kumar, M., Ghani, R., and Mei, Z. S. (2010). Data mining to predict and prevent errors in health insurance claims processing.ACM *16th International Conference on KnowledgeDiscovery and Data Mining,*pp. 65-74. Available from: http://dx.doi.org/10.1145/1835804.1835816

[25] Kirlidog, M., and Asuk, C. (2012).A fraud detection approach with data mining in health insurance.*Procedia-Social and Behavioral Sciences,* **62***:* 989-994. http://dx.doi.org/10.1016/j.sbspro.2012.09.168

[26] Anwar, S., Zain, J. M., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., and Chang, V. (2017). From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. *MDPI Algorithms*, **10**(2):1-24, DOI: 10.3390/a10020039

[27] Ekin, T., Leva, F., Ruggeri, F., and Soyer, R. (2013). Application of bayesian methods in detection of healthcare fraud. *Chemical Engineering Transactions,* **33**:151- 156.DOI: 10.3303/CET1333026

[28] Cortes, C., and Vapnik, V., (1995). Support vector network, *Machine Learning,* **20(**3): 273-297. DOI:https://doi.org/10.1023/A:1022627411411

[29] Chiu, N.H., and Guao, Y.,Y. (2008). State classification of CBN grinding with support vector machine.*Journal of Material Processing Technology*, **201**:601-605.

[30] Elmi, H.E., Sallehuddin, R., Ibrahim, S., and Zain, A.M. (2014). Classification of sim box fraud detection using support vector machine and artificial neural network, *International Journal of Innovative Computing*, **4** (2): 19-27.

[31] Demla, N.,and Aggarwal, A., (2016). Credit card fraud detection using svm and reduction of false alarms.*International Journal of Innovations in Engineering and Technology*, **7(**2): 176-182.

[32] Abdelhamid, D., Khaoula, S., and Atika, O. (2014). Automatic bank fraud detection using support vector machines. *International Conference on Computing Technology and Information Management*, pp. 10-17, Dubai, UAE.

[33] Quinlen, J.R., (1986). Introduction of decision trees, *Machine Learning,* **1**: pp. 81-106.

[34] Han J. and Kamber, M. (2011). Data mining concepts and techniques, *Elsevier*, p. 744, Morgan Kaufmann.

[35] Kotsiantis, S.B. (2007). Supervised machine learning: A review of classification techniques. *Informatica,* **31**: 249-268.

[36] Williams, G.J., and Huang, Z. (1997). Mining the knowledge mine: The hot spots methodology for mining large real world databases. *Australian Joint Conference on Artificial Intelligence*, pp. 340-348.

[37] Liou, F. M., Tang, Y. C., and Chen, J. Y. (2008). Detecting hospital fraud and claim abuse through diabetic outpatient services. *Health Care Management Science, **11***(4): 353-358.Available from: http://dx.doi.org/10.1007/s10729-008-9054-y

[38] Shin, H., Park, H., Lee, J., and Jhee, W. C. (2012). A scoring model to detect abusive billing patterns in health insurance claims.*Expert Systems with Applications*,**39**(8), 7441-7450 Available from: .http://dx.doi.org/10.1016/j.eswa.2012.01.105.

[39] Bhavsar, H., and Ganatra, A. (2012). A comparative study of training algorithms for supervised machine learning.*International Journal of Soft Computing and Engineering,* **2**(4): 2231-2307.

[40] Bhavsar, H., and Ganatra, A. (2016). An empirical evaluation of data mining classification algorithms. *International Journal of Computer Science and Information Security (IJCSIS),***14**(5): 142-150.

[41] Quinlan, J.R. (1979), "Discovering rules by induction from large collections of examples", D. Michie ed., Expert Systems in the Microelectronic age, pp. 168-201.

[42] Quinlan, J.R. (1993). C4.5: Programs for machine learning. Morgan Kaufmann, San Francisco.

[43]Rosenblatt, F., (1962). Principles of Neurodynamics, Spartan, New York.

[44] Duda, R. O. and Hart P. E. (1973). Pattern Classification and Scene Analysis. New York: John Wiley & Sons.

[45] Cover, T., Hart, P. (1967), Nearest neighbor pattern classification. IEEE Transactions on Information Theory, 13(1): 21–7.

[46] Vapnik, V. (1995), The Nature of Statistical Learning Theory}. Springer Verlag.

[47] Zhu, X. (2008). "Semi-Supervised Learning Literature Survey," University of Wisconsin, Madison.

[48] Brabazon, A., Cahill, J., Keenan, P., and Walsh, D. (2010). "Identifying Online Credit Card Fraud using Artificial Immune System," in *IEEE Congress on Evolutionary Computation (CEC)*, Dublin, 2010.

[49] Tuo, J., Red, S., Lid, W., Li, X., Li, B. and Lei, L. (2004). Artificial Immune System for Fraud Detection, in *IEEE International Conference on Systems, Man and Cybernetics*, China.

[50] Graaff, A. J., Engelbrecht, A. P. (2011). The Artificial Immune System for Fraud Detection in the Telecommunications Environment.

[51] Wong, N., Ray, P., Stephens, G., and Lewis, L. (2012). "Artificial immune systems for the detection of credit card fraud". *Information Systems,* Volume 22.

[52] Ngai, E., Hu, Y. Wong, Y. Chen, Y., and Sun, X. (2011). "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decision Support Systems,* pp. 559-569.

[53] Yu, W. F., and Wang, N. (2009). Research on Credit Card Fraud Detection Model Based on Distance Sum, *International Joint Conference on Artificial Intelligence,* pp. 353-356.

[54] Hand, D. J. (2010). Fraud Detection in Telecommunications and Banking: Discussion of Becker, Volinsky, and Wilks (2010) and Sudjianto et al. (2010), *Technometrics,* vol. 52, no. 1, pp. 34-38, 2010.

[55] Weston, D. J., Hand, N. M., Adams, C., Whitrow, C. and Juszczak, P. (2008)."Plastic card fraud detection using peer group analysis," *Springer-Verlag,* pp. 45-62.

[56] Srivastava, A. Kundu, A. Sural, S. and Majumdar, A.K. (2008). "Credit Card Fraud Detection Using Hidden Markov Model," *IEEE Transactions On Dependable And Secure Computing,* Vol. 5, no. 1, pp. 37-48. [3] URL Date Stamp Time Stamp GMT and dd/mm/yyyy

[57] Maes, S. Tuyls, K. Vanschoenwinkel, B. and Manderick, B. (2002). Credit Card Fraud Detection Using Bayesian and Neural Networks," Vrije Universiteit Brussel - Department of Computer Science, Belgium.

[58] Gadi, M.F.A. Wang, X., and Pereira do Lago, A. (2008). "Credit Card Fraud Detection with Artificial Immune System," *Springer-Verlag Berlin Heidelberg,* pp. 119-131.

[59] Ang, R. P. and Goh, D.H. (2013). Predicting Juvenile Offending: A Comparison of Data Mining Methods, *International Journal of Offender Therapy and Comparative Criminology,* vol. 57, no. 2, pp. 191-207.

[60] Major, J. A., and Riedinger, D.R. (2002). "EFD: A hybrid knowledge/statistical-based system for the detection of fraud. *Journal of Risk and Insurance*, **69**(3): 309-324.

[61] Hansen, L.K., and Salamon, P. (1990). Neural network ensembles. *IEEE Transactions on Pattern Analysis and Machine Intelligence,***12**(10): 993–1001.

[62] Schapire, R.E. (1990). The strength of weak learnability.*Machine Learning,* **5**(2): 197–227.

[63] Zhou, Z.H., Jiang, Y., and Chen, S.F. (2003).Extracting symbolic rules from trained

neural network ensembles.*AI Communications*,**16(**1):3–15.

[64] Wolpert, D.H. (1992). Stacked generalization. *Neural Networks* **5**(2) (1992) 241–260.

[65] Breiman, L. (1996). Bagging predictors, *Machine Learning* **24**(2): 123–140.

[66] Freund,Y., and Schapire, R. E. (1996). Experiments with a new boosting algorithm. *Proceedings of the Thirteenth International Conference on Machine Learning*, pp. 148 – 156.

[67] Sun, Y., Kamel, M. S., Wong, A. K., and Wang, Y. (2007). Cost-sensitive boosting for classification of imbalanced data.*Pattern Recognition*, **40(**12): 3358-3378.

[68] Ali, A., Shamsuddin, S. M., and Ralescu, A. L. (2015). Classification with class imbalance problem: A review. *International. Journal of Advanced Soft ComputingAppllications,***7** (3): 176-204.

[69] He, H., and Garcia, E. A. (2009). Learning from imbalanced data. *IEEE Transactions on Knowledge and Data Engineering*, **21**(9): 1263-1284.

[70] Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., Geraili, B., Nasiri, M., and Arab, M. (2015). Using data mining to detect health care fraud and abuse: A review of literature. *Global Journal of Health Science*.**7(**1):194-202.

[71] Seemakurthi, P., Zhang, S. and Qi, Y. (2015). Detection of fraudulent financial reports with machine learning techniques. *Systems and Information Engineering Design Symposium*, pp. 358-361.

[72] Manjunath, K.V., (2015). Data mining techniques for anti money laundering. *International Journal of Advanced Research in Science, Engineering and Technology,* **2(**8): 819-823.

[73] Rohit, K.D., and Patel, D.B. (2015). Review on detection of suspicious transaction in anti-money laundering using data mining framework, *International Journal for Innovative Research in Science & Technology*,**1(**8): 129-133.

[74] West, J., Bhattacharya, M., and Islam, R. (2014). Intelligent financial fraud detection practices: An investigation, *International Conference on Security and Privacy in Communication Systems*, pp. 186-203. DOI: 10.1007/978-3-319-23802-9_16.

[75] Kirkos, E., Spathis, C., and Manolopoulos, Y. (2007).Data mining techniques for the detection offraudulent financial statements. *Expert Systems with Applications*.**32(**4): 995-1003.

[76] Abbasi, A., Albrecht, C., Vance, A., and Hansen, J. (2012). Metafraud: A meta-learning framework for detecting financial fraud. *MIS Quarterly*, **36** (4): 1293-1327.

[77] West, J., and Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review.*Computers & Security,* **57**: 47-66.

[78] Seeja, K.R., and Zareapoor, M. (2014). FraudMiner: A novel credit card fraud detection model based on frequent itemset mining, *The Scientific World Journal*, **1**: 1-10. DOI: http://dx.doi.org/10.1155/2014/252797.

[79] Choi, K., Kim, G., Suh, Y. (2013). Classification model for detecting and managing credit loan fraud based on individual-level utility concept, *Data Base for Advances in Information Systems,* **(44)**3, pp. 49-67.

[80] Xuan, S., Liu, G., Li, Z., Zheng, L., Wang, S., Jiang, C., (2018). Random forest for credit card fraud detection, *15th IEEE International Conference on Networking, Sensing and Control*pp. 1-6.

[81] Abid, L., Masmoudi, A., and Zouari-Ghorbel, S. (2016). The consumer loan's payment default predictive model: An application in a Tunisian commercial bank. *Asian Economic and Financial Review*, **6**(1): 27-42.

[82] Rawate, K.R., and Tijare, P. A. (2017). Review on prediction system for bank loan credibility, *International Journal of Advance Engineering and Research Development,* **4(**12): 860-867.

[83] Boateng, E.Y., and Oduro, F.T. (2018).Predicting microfinance credit default: a study of nsoatreman rural bank, Ghana.*Journal of Advances in Mathematics and Computer Science (JAMCS),* **26(**1): 1-9.

[84] Chen, S., Goo,Y.J, and Shen, Z. (2014).A hybrid approach of stepwise regression, logistic regression, support vector machine, and decision tree for forecasting fraudulent financial statements. *The Scientific World Journal*, (1):1-9.

[85] Rao, V.M., and Singh, Y.P. (2013). Decision tree induction for financial fraud detection using ensemble learning techniques. *Proceeding of the International Conference on*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Artificial Intelligence in Computer Science and ICT, pp. 25 -26.

[86] Witten, I.H., Frank, E., and Hall, M.A. (2011). Data mining: Practical machine learning tools and techniques (3rd ed.), p. 664. *Elsevier*. Available from: https://www.elsevier.com/books/data-mining-practical-machine-learning-tools-and-techniques/witten/978-0-12-374856-0

[87] Freund,Y., and Schapire, R. E. (1996). Experiments with a new boosting algorithm. *Proceedings of the Thirteenth International Conference on Machine Learning*, pp. 148 – 156.

[88] Bian, Y., Cheng, M., Yang, C., Yuan, Y., and Li, Q. (2016). Financial fraud detection: A new ensemble learning approach for imbalanced data. *Pacific Asia Conference on Information Systems* (*PACIS) 2016 Proceedings*,pp. 1-11. Available from: http://aisel.aisnet.org/pacis2016/315/

[89] Kitchenham, B. and Charter, S. (2007). "Guidelines for Performing Systematic Literature Reviews in Software Engineering", v. 2.3, Technical Report, Keele University and University of Durham.

[90] Host, M., and Orucevic-Alagic, A. (2013)."A Systematic Review of Research on Open Source Software in Commercial Software Product Development." http://www.bcs.org/upload/pdf/ewic_ea10_session5paper2.pdf.

[91] Jalili, S. and Wohlin, C. (2010). Agile Practices in Global Software Engineering- A Systematic Map, International Conference on Global Software Engineering (ICGSE), 2010, Princeton, NJ.

[92] Brinkel, J., Kraemer, A., Krumkamp, R., May, J., Fobil, J. (2014). Mobile phone-based mHealth approaches for public health surveillance in sub-Saharan Africa: A systematic review, *International Journal of Environmental Research and Public Health*, 11: 11559-11582; doi:10.3390/ijerph111111559.

[93] Rao, V.M., and Singh, Y.P. (2013). Decision tree induction for financial fraud detection using ensemble learning techniques. *Proceeding of the International Conference on Artificial Intelligence in Computer Science and ICT*, pp. 25 -26.

[94] Eweoya, I.O. and Daramola, O. (2015), A systematic literature review of mobile cloud computing, *International Journal of Multimedia and Ubiquitous Engineering.* www.sersc.org/journals/IJMUE/vol10_no12_2015/15.pdf

[95] Ayo, C.K., Oni, A.A., Adewoye, O.J. and Eweoya, I.O. (2015). E-banking users' behaviour: e-service quality, attitude, and customer satisfaction, *International Journal of Bank Marketing.* http://www.emeraldinsight.com/doi/abs/10.1108/IJBM-12-2014-0175?af=R

[96] Azeta., A.,A., Eweoya, I. O. and Samuel Ojumah, S. (2014). Enhancing educational learning with social network platform, *6th International Conference On Adaptive Science & Technology (ICAST), IEEE,* 2014. *ieeexplore.ieee.org/iel7/7056705/7068059/07068143.pdf*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

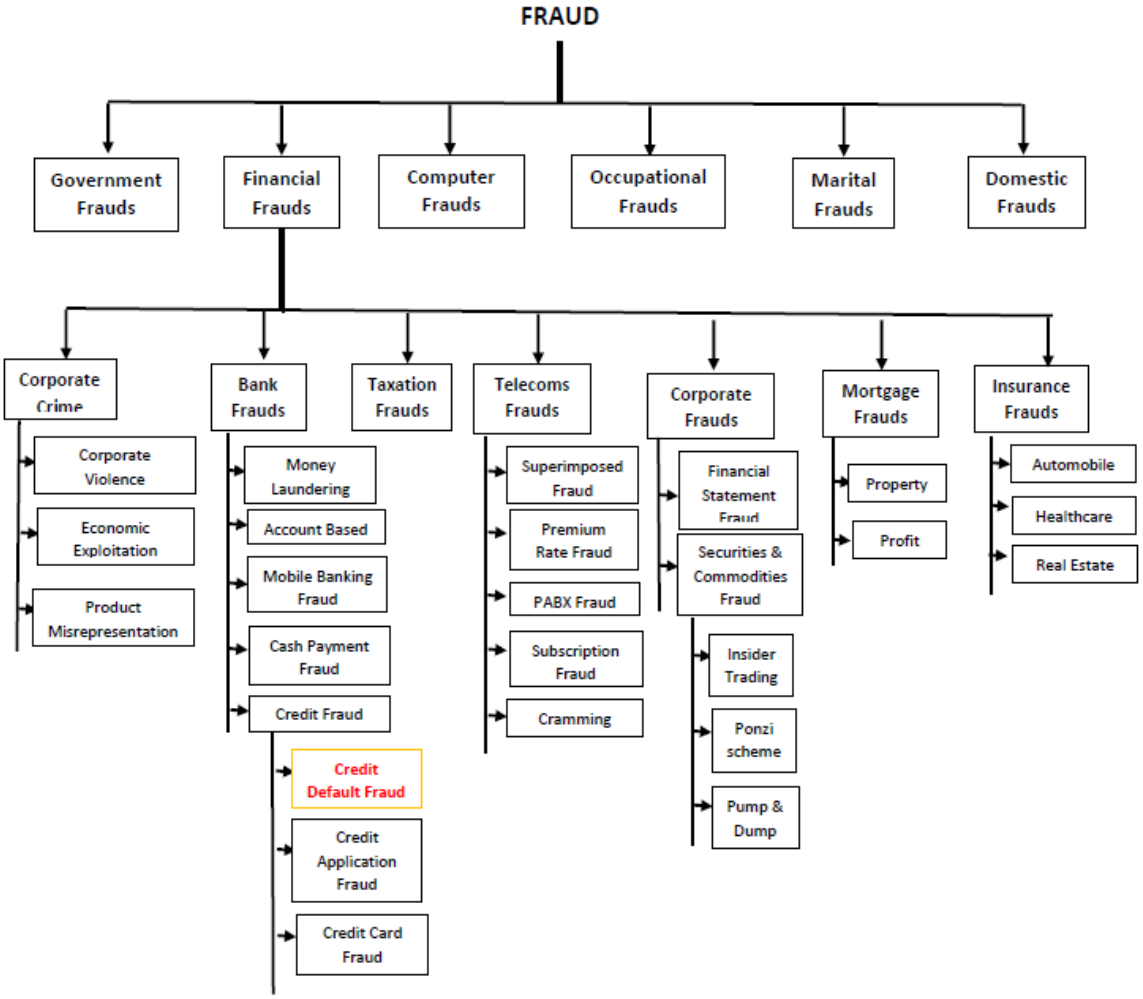

Figure 1: Types of fraud (Potamitis, 2013)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

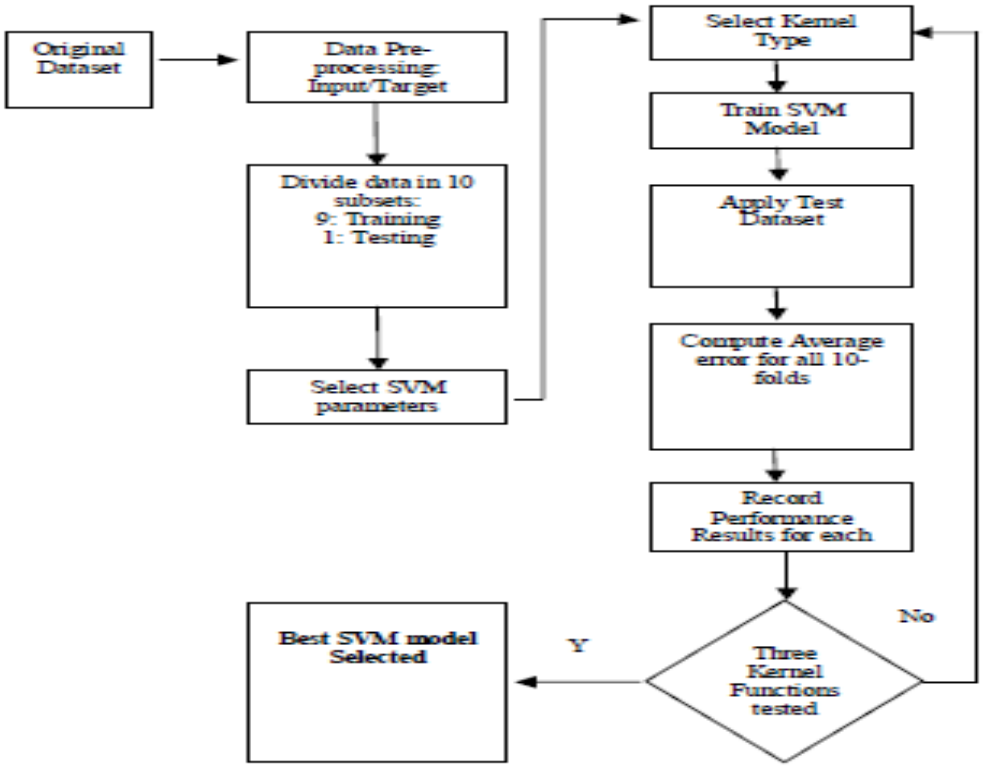

Figure 2: A Sample of an SVM Implementation (Elmi et al., 2014).

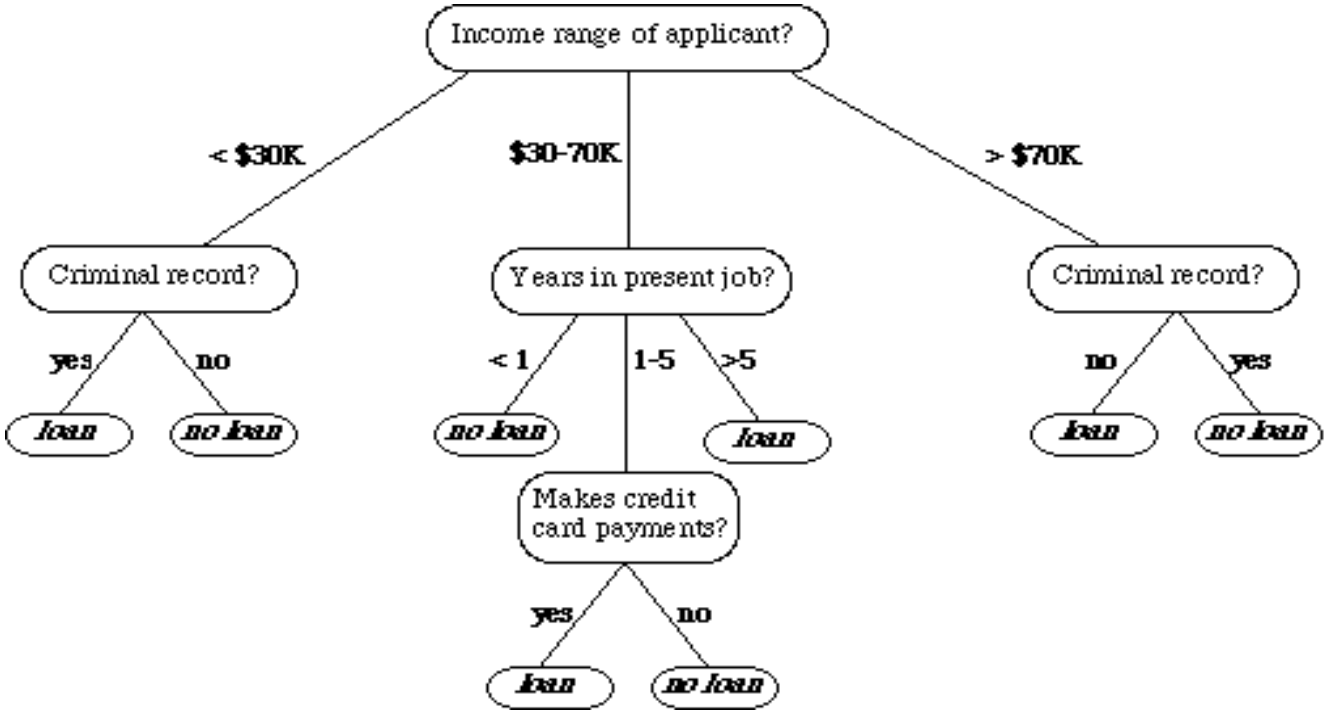

Figure 3: Bank loan application decision tree

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

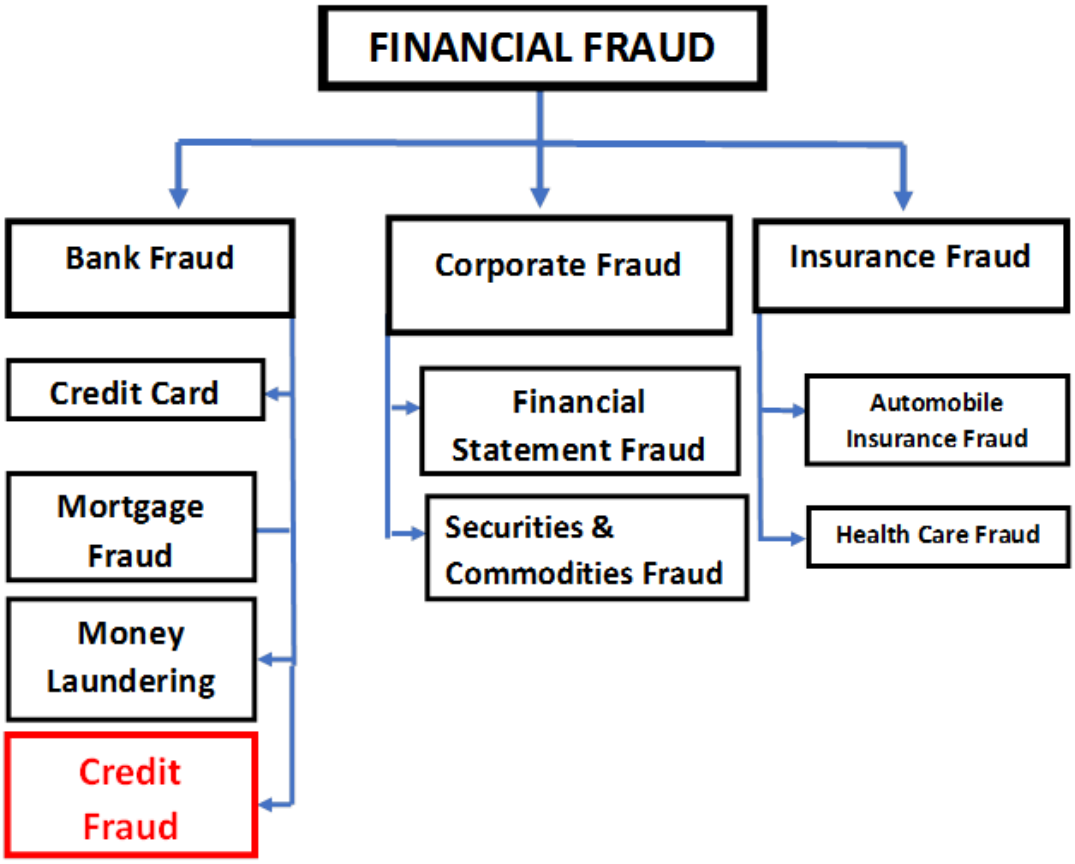

Figure 4: Financial fraud categories (West et al., 2014).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

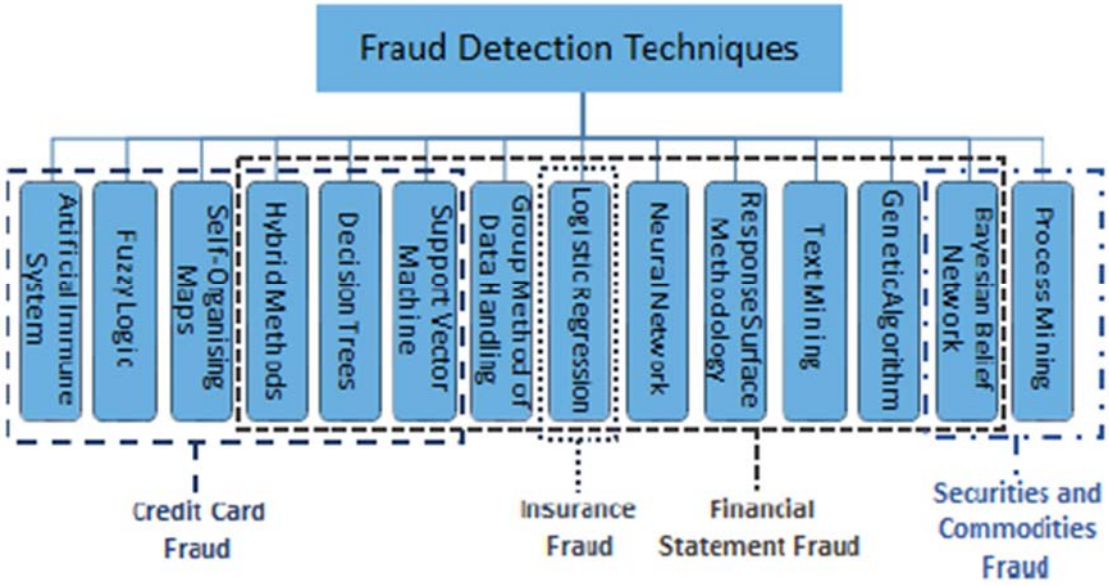

Figure 5: Detection algorithms used for some fraud categories (West et al., 2014).

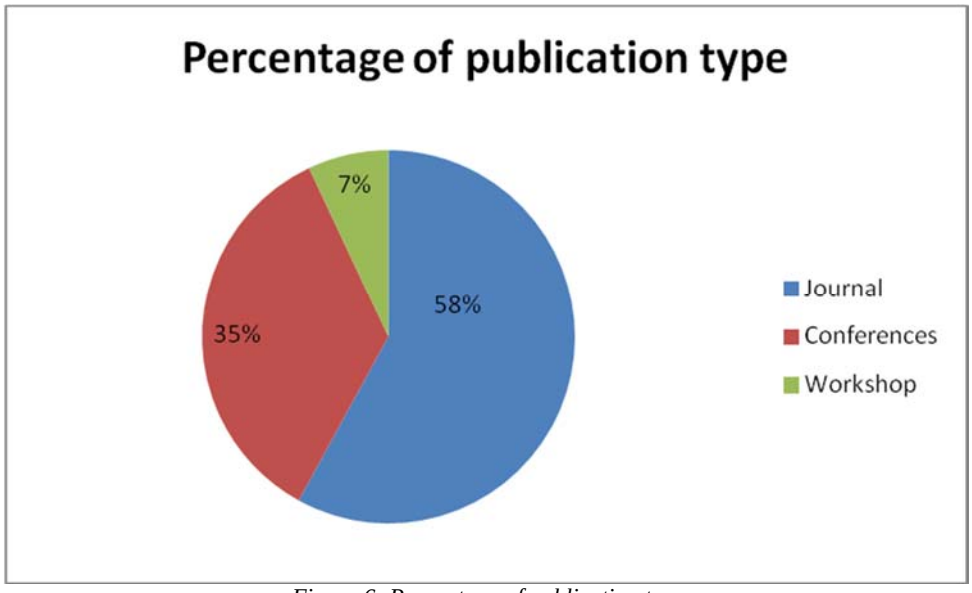

Figure 6: Percentage of publication type

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Comparison of common classification techniques (Bhavsar and Ganatra, 2012; 2016).

	Decision Trees	**Neural Networks**	**Naïve Bayes**	**K-Nearest Neighbor**	**Support Vector Machine**
Authors	**Quinlan (1979; 1993)**	**Rosenblatt (1962)**	**Duda and Hurt (1973)**	**Cover and Hart (1967)**	**Vapnik (1995)**
Accuracy in general	**	***	*	**	****
Speed of learning	***	*	****	****	*
Speed of classification	****	****	****	*	****
Missing values tolerance	***	*	****	*	**
Tolerance to irrelevant attributes	***	*	**	**	****
Tolerance to redundant attributes	**	**	*	**	***
Tolerance to highly interdependent attributes	**	***	*	*	***
Dealing with discrete/binary/continuous attributes	All	Not discrete	Not continuous	All	Discrete
Tolerance to noise	**	**	***	*	**
Dealing with danger of overfitting	**	*	***	***	**
Attempt for incremental learning	**	***	****	****	**
Explanation ability, knowledge transparency, classification	****	*	****	**	*
Support multi-classification	****	Naturally extended	Naturally extended	****	Binary classifier

*** = Average, ** = Good, *** = Very good, **** = Excellent**

Table 2: The basic inclusion and exclusion considerations for this study

	Inclusion
1.	Peer-reviewed papers, and conference proceedings
2.	English language must be the language used
3.	Fraud, credit fraud, bank credit fraud or machine learning must be in the paper topic
4.	When same research was discovered to have been published twice, and the authors are not different, the latest of the two was chosen.
5.	Only publications from conferences, journals, academic workshops were chosen.
6.	Publication year limitation of 2001 to 2018
7.	Limit by subject area (Computer Science and IT).
8.	Year of publication must be within 2001 to 2018
	Exclusion
1.	Technical reports, hypothetical reports, workshops on fraud prediction.
2.	Theoretical literature or critiques
3.	Newspapers report or television commentary
4.	Editorial discussion that discussed the field to argue for research requirement
5.	Studies only mentioned through web pages but with insignificant technical information
6.	Publications that focus on automated teller machine fraud, mortgage fraud, or bank fraud were excluded because they represent another concept, although bank fraud is the general name as every credit is linked to a bank.
7.	Journal articles that are not peer-reviewed but from professional bodies

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: Systematic literature and information search strategy.

Step	Description	Details
1.	Bibliographic databases	General bibliographic databases The subject-specific bibliographic database IEEEXplore.
2.	Full-text journals, non-bibliographic databases	The digital library, published material and technical information in full text. Google Scholar, Researchgate, ScienceDirect, Scopus, ACM Digital Library, and SpringerLink.
3.	Open search on websites	Visiting relevant websites in the domain of study
4.	Information request via Email to specified Organizations	Establishing contact with companies or personnel of certain organizations for required helpful information to the research
5.	Personal information request through electronic mails to authors of impactful publications for full texts, additional information, hints and expertise.	Request for full text of publications not available without a particular subscription or payment
6.	A critical look into reference lists of impactful publications	Some consulted crucial publications pointed to important references that led to relevant papers

Table 4: Distribution Of Papers Over The Studied Years

Year	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	Total
No	1	3	1	1	1	1	3	7	3	3	4	8	8	6	7	6	5	2	80