Int J Syst Assur Eng Manag (November 2017) 8(Suppl. 2):S937–S953
DOI 10.1007/s13198-016-0551-y

ORIGINAL ARTICLE

A survey of machine-learning and nature-inspired based credit card fraud detection techniques

Aderemi O. Adewumi[1] · **Andronicus A. Akinyelu**[1]

Received: 17 March 2016 / Revised: 4 May 2016 / Published online: 19 December 2016

Abstract Credit card is one of the popular modes of payment for electronic transactions in many developed and developing countries. Invention of credit cards has made online transactions seamless, easier, comfortable and convenient. However, it has also provided new fraud opportunities for criminals, and in turn, increased fraud rate. The global impact of credit card fraud is alarming, millions of US dollars have been lost by many companies and individuals. Furthermore, cybercriminals are innovating sophisticated techniques on a regular basis, hence, there is an urgent task to develop improved and dynamic techniques capable of adapting to rapidly evolving fraudulent patterns. Achieving this task is very challenging, primarily due to the dynamic nature of fraud and also due to lack of dataset for researchers. This paper presents a review of improved credit card fraud detection techniques. Precisely, this paper focused on recent Machine Learning based and Nature Inspired based credit card fraud detection techniques proposed in literature. This paper provides a picture of recent trend in credit card fraud detection. Moreover, this review outlines some limitations and contributions of existing credit card fraud detection techniques, it also provides necessary background information for researchers in this domain. Additionally, this review serves as a guide and stepping stone for financial institutions and individuals seeking for new and effective credit card fraud detection techniques.

Keywords Credit card fraud · Electronic transactions · Machine learning · Nature-inspired techniques · Cybercriminals

1 Introduction

Credit card fraud can be defined as illegal use of credit card information for online purchase. Credit card transactions are done physically or virtually (Zareapoor et al. 2012). Physical transactions refers to transactions involving physical interaction with seller. Users are required to present a physical card at the point of purchase (Zareapoor et al. 2012). Virtual transactions refers to transactions performed over the internet or telephone (Zareapoor et al. 2012). It require users to provide certain card information (such as CVV number, password, security question, etc.) for online purchases (Zareapoor et al. 2012). The invention of credit cards has not only made online transactions seamless, easier, comfortable and convenient, it has also provided new fraud opportunities for criminals, and increased the rate of fraud (Maes et al. 2002) (Pun 2011). The effect of credit card fraud is alarming and it is has affected the global economy in measurable ways. Millions of US dollar has been lost by many individuals and companies. In 2009, the total value of online order (for goods and services only) was approximately US$15 billion (Pun 2011). Moreover, 84% of these orders were paid online (Pun 2011). In 2013, fraud was estimated to cost US retailers about $23 billion, and in 2014, the cost of fraud rose to approximately $32 billion (Insider 2015). Weak

✉ Aderemi O. Adewumi
adewumia@ukzn.ac.za

Andronicus A. Akinyelu
akinyelu.ayobami@gmail.com

[1] School of Mathematics, Statistics and Computer Science, University of Kwa-Zulu Natal, University Road, Westville, Private Bag X 54001, Durban 4000, South Africa

security of credit and debit card is one of the major cause of credit card fraud. In the UK, card-not-present fraud is estimated to cost £183.2 million in year 2011 (Wong et al. 2012). Also, VISA processes approximately US$3 trillion worth of transaction every year, and for every $100, seven cent goes to irregular transactions (VISA 2005a). Every credit card user stand the risk of falling victim to card-not-present fraud and retailers bears the cost of irregular transactions (FFA 2015).

Credit card fraud detection is a classification problem (Wong et al. 2012). Credit card numbers are generated using Luhn algorithm (Wong et al. 2012). The algorithm does not categorically protect users from online fraud, it essentially helps in authenticating data input from users (Wong et al. 2012). Some small scale companies use manual authentication methods, including: validation of phone numbers, physical address, secret question and answer (Wong et al. 2012). However, this methods may not be feasible for large scale companies, they are expensive and inefficient (Wong et al. 2012). Furthermore, most online merchants now use Card Verification Value (CVV2) as an additional security measure for approval of card-not-present transactions (Wong et al. 2012). Although, this additional security measure has reduced card-not-present fraud to a reasonable minimum, it does not prevent fraud that occurs due to lost or stolen card (Wong et al. 2012). Address Verification Service can be used to combat card-not-present fraud. It is an electronic service that verifies transactions by using shipping address details of card owners (Wong et al. 2012). This method reduces fraud, however, it lead to loss in sales, because, not all customers are willing to ship purchased items to their billing address (Wong et al. 2012). Furthermore, MasterCard and VISA card has introduced a 3-D secured protocol for online banking, they include MasterCard Secure Code and Verified by VISA (Wong et al. 2012). These protocols use a digital certificate to authenticate online merchants and password to authenticate customers (Wong et al. 2012).

Fraudsters mostly use internet to commit fraud, because their identity and location can be easily concealed (Sahin and Duman 2011). Loss incurred from credit card fraud affects both customers and merchants. Although, merchants bear most of the loss, customers are made to pay higher interest rates and higher fees for membership (Maes et al. 2002). Merchants also reduce their promos and incentives (Maes et al. 2002). Fraud detection is very essential in reducing losses incurred by financial institutions and individuals. The primary objective of fraud detection systems is to identify fraud promptly (Pun 2011). In a credit card transaction, four parties are typically involved, namely: card holder, merchant, financial institution and the VISA center (Ehramikar 2000). All these parties require security. Most of the existing fraud detection systems are rule-based system (Duman and Ozcelik 2011). Rules are developed based on known patterns, hence these systems are only capable of detecting known fraudulent patterns; they are not capable of detecting unknown or emerging patterns. Averagely, it takes approximately 72 h for a fraudulent transaction to be discovered (Quah and Sriganesh 2008). Duman and Ozcelik (2011) alluded that rule based systems are only useful for counterfeit card fraud detection; they are not useful for lost/stolen card fraud detection. To address this issue, fraud detection system developers should take into cognizance, fraudster behavior and card user behavior (Duman and Ozcelik 2011).

2 Credit card fraud detection

Fraud detection is a data mining problem with an aim of segregating transactions into two classes – legitimate and fraudulent (Duman and Ozcelik 2011). Recent fraud detection systems used by merchants and banks are designed to verify transactions by checking spending patterns and behavior of customers (Quah and Sriganesh 2008). To achieve this, fraud detection systems use prediction algorithms to classify pattern observations (Maes et al. 2002). A transaction will be labeled fraudulent if the system observes a deviation in the normal spending pattern of a user. The following are some techniques used in credit card detection (Quah and Sriganesh 2008):

(a) Transaction verification through Address Verification System (AVS) using customer zip code.
(b) Transaction verification through Card Verification Method (CVM) using a secret number entered by the customer.
(c) Transaction verification through Personal Information Number (PIN) using a secret number to be provided by the customer during transactions.
(d) Transaction verification through biometrics using fingerprint.

Two major methods used to handle fraud include: fraud prevention and fraud detection (Sahin and Duman 2011). Fraud prevention aims to stop fraudulent activity from taking place (Sahin and Duman 2011). Fraud detection aims to identify fraudulent transactions, and in turn prevent authorization of the transaction (Sahin and Duman 2011). Fraud detection commences after a system fails to stop fraudster from initiating a transaction, that is, after the fraudster has started the transaction. Most of the existing fraud detection mechanism, such as Chip and PIN has failed to handle fraud effectively (Sahin and Duman 2011).

2.1 Characteristics of a good fraud detection system

A good fraud detection solution should be capable of reducing high risk fraud to the barest minimum (Duman and Ozcelik 2011). High risk fraud refers to fraud that leads to huge money loss. When a card is stolen, its entire credit limit is habitually the major target. Fraudsters exhaust the credit limit within 4–5 transactions (Duman and Ozcelik 2011). The higher the credit limit, the higher the loss. Misclassification cost of each transaction varies, hence, good credit card fraud detection systems should give priority to transactions with higher misclassification cost.

The following are some other characteristics of a good fraud detection system (Maes et al. 2002):

(a) Skewed Distribution: A good fraud detection system should be capable of handling skewed distributions. This is because only few fraudulent transactions are in record. This challenge can be handled by dividing the training dataset into different parts having a reduced skewed distribution.
(b) Noise: A dataset is said to be noisy if it contains corrupted or erroneous data. A good fraud detection system should be able to handle noise. Generally, noise affects the performance of a classifier.
(c) Overlapping Data: A good fraud detection system should be able to detect fraudulent transactions that look very similar to legitimate transactions.
(d) Dynamism: Techniques used by fraudsters change overtime. A good fraud detection system should be dynamic; it should be able to adjust to changes in fraudulent patterns.
(e) Good Classification Metrics: The classification metric used in evaluating fraud detection techniques should to be chosen carefully. This is because; metrics like classification accuracy is not suitable for skewed distribution.

2.2 Challenges in credit card fraud detection

The following are some frequently encountered problem in fraud detection (Sahin and Duman 2011; Gadi et al. 2016):

(a) Data imbalance: Due to privacy issue, number of available data is limited. Furthermore, the few available datasets are imbalanced. They contain more legitimate transactions than fraudulent transactions.
(b) Variability in misclassification cost: The misclassification cost associated with stolen cards varies. This is because of the difference in the card limit associated with each card.
(c) Model durability: Fraud patterns changes over time. Rule-based systems are not robust enough to effectively handle emerging patterns.
(d) Pattern matching is very difficult. This is because, some fraudulent pattern looks very similar to normal patterns (Sahin and Duman 2011).
(e) High search space dimensionality. The number of transactions to be processed by fraud detection systems is usually very large. Some fraud detection systems process millions of transactions.
(f) Robustness of the fraud detection model. Developing a model that can handle the vast changes in fraudulent techniques is not an easy task.

Credit card transactions has two unique peculiarities (Patidar and Sharma 2011). The first peculiarity is centered on the number of credit card transactions. The number of credit card transactions processed at a particular time is numerous (Patidar and Sharma 2011). The second unique attribute is time. Card users have limited time to either reject or accept a given transaction (Patidar and Sharma 2011). On a daily basis, millions of visa card operations are performed by users worldwide, and 98% of these transactions are online based (Patidar and Sharma 2011). Security of credit cards depends on card owners. It depends on how efficient a user can secure his card and card number from theft.

2.3 Features used in credit card detection

Features used in constructing classifiers for credit card detection systems are divided into three (Quah and Sriganesh 2008):

(a) Features related to accounts: they include; account number, account type (dollars, rands, etc.), date of account opening, date of last transaction (debit or credit), and balance available in account, card expiry date, etc.
(b) Features related to transactions: Transaction-specific features include: transaction reference number, account number, type of transaction (debit or credit), currency of transaction, timestamp of transaction, terminal (i.e. POS) reference number, etc.
(c) Features related to customers: they include: customer number, branch of customer, type of customer (high profile, low profile, etc.)

The following are some fraudulent patterns that characterizes fraud (Quah and Sriganesh 2008).

(a) Change of PIN before the initiation of a high-profile transaction.
(b) Invalid number of login attempts before initiating a transaction.

(c) Sudden activation of an Inactive (or dormant) account.
(d) Transactions emanating from locations that are already blacklisted.
(e) High volume transactions initiated from a region different from the person that initiates the transaction.
(f) Card replacement request, coupled with simultaneous card transaction.

2.4 Techniques used by fraudsters

The following are some commonly used online fraud techniques (Patidar and Sharma 2011):

(a) Site Cloning: this involves designing the exact duplicate of web sites. Users ignorantly visit cloned websites and enter their card information.
(b) Credit card generators: Some fraudsters use credit card generators for fraudulent activities. These generators are computer programs capable of generating credit card numbers and expiry dates. A list of card numbers is usually generated for the account of one card holder.
(c) Account Takeover: this occurs when fraudsters use stolen information (card number, card number, CVV number, etc.) illegally obtained from card holders to control account of users. In some instances, fraudsters (posing as the card owner) can send a message to a card issuer requesting for change of address and change of card. In other instances, fraudsters can use stolen information (such as username and password) to logon to customer account and change customer details making it difficult for the original account owner to recover the account.
(d) Fake Card: Fraudsters clones stolen cards and use them for fraudulent transactions. Fraudsters use different cloning methods. In some cases, fraudsters use magnet to erase the magnetic strip in cards. Afterwards, the information on the card will be changed to that of a valid user. In some other instance, fraudsters use skimming devices (containing electronic magnetic strip reader) to copy the magnetic stripe information of a valid card into a fake card. Sometimes the transfer of information is done without the knowledge of card owners, because, fraudster can put the skimming devices in their pocket and move closer to the place where the valid card is kept. Afterwards, the fraudster will then use the cloned card to perform card-not-present transactions
(e) Mail Theft: Some fraudsters divert mails containing card number that are newly supplied.
(f) Fraudsters also gather information through cloned website (i.e. phishing) or from card issuer employees.

Credit card related fraud can be divided into three groups (Patidar and Sharma 2011):

(a) Fraud perpetrated with physical card.
(b) Fraud perpetrated on merchant. This type of fraud is perpetrated either by the merchant owners (called merchant collusion) or the merchant employees (triangulation). In merchant collusion, merchant owners collide with each other to steal money from their customers. Stolen information of card holders are obtained and given to fraudsters.
(c) Fraud perpetrated over the internet: Here, fraudsters illegally obtain card holder information and use it to purchase items online.

2.5 Credit card transaction processing flow

Below is a flow of credit card transactions (Ehramikar 2000). The flow is also depicted by the flowchart in Fig. 1.

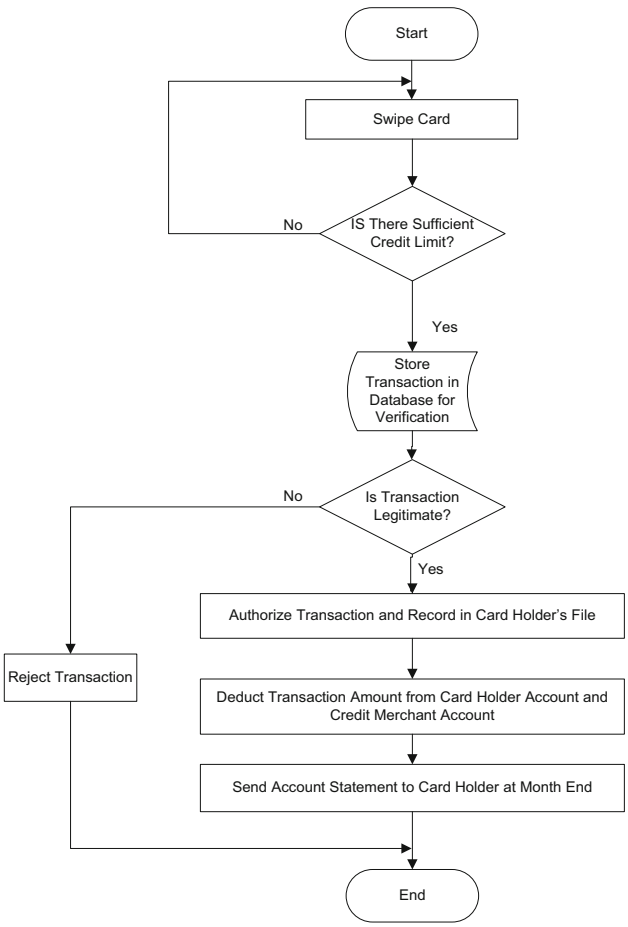

Fig. 1 Flowchart for credit card transaction

(a) Firstly, user is expected to swipe a card (for virtual transaction) or enter card details (for physical transactions).
(b) Furthermore, the transaction is approved if the card information is verified ok and if there is sufficient credit limit.
(c) Afterwards, the transaction request is sent to a file. The request stays in the file for 5 days. During this period, the transaction is verified by the merchant.
(d) Afterwards, if the transaction is legitimate, it is authorized and recorded in the cardholder's file. Transaction authorization is an important part of a transaction. It is also the first level of security. The credit card limit of cardholders is regulated at this level.
(e) After authorization, transaction amount is deducted from the account balance of cardholder. The deducted amount will be credited to merchants account.
(f) At the end of the month, the financial institution will send a statement of account containing the list of transactions that have been performed by the user. The statement contains the outstanding balance. The user is then expected to pay the total balance.

3 Machine learning and nature inspired based fraud detection survey

Some common types of fraud include: credit card fraud, computer intrusion, money laundering (Sahin and Duman 2011). This section present a survey of some recent credit card fraud detection techniques proposed in literature. Popular Nature Inspired (NI) and Machine Learning (ML) credit card fraud detection techniques used in literature include: HMM, NN, SVM, Artificial Immune System (AIS) and GA. Other techniques include: meta-learning, frequent pattern learning, ontology and decision support system. These techniques are used alone or hybridized with other techniques to construct robust classifiers. In some studies, NI algorithms were hybridized with ML algorithms, and in other studies, two or more ML algorithms are combined (called ensemble). Generally, hybridized techniques performs better than stand-alone techniques.

Stand-alone ML-based credit card fraud detection techniques used in literature include: NN, HMM, Meta-learning, SVM, Frequent itemset mining, ontology, decision support system and Fisher Discriminant Analysis. Stand-alone NI-based credit card fraud detection techniques used in literature include: AIS and GA. Furthermore, hybridized techniques used in literature include: HMM and K Nearest Neighbor (KNN), Artificial Neural Network (ANN) and simulated annealing, decision tree and SVM, Bayesian network and NN, transaction aggregation and logistic regression. Few studies used fisher discriminant analysis, simulated annealing, ontology and frequent itemset mining. Table 1 gives a summary of the surveyed techniques. This section presents a survey of some these techniques. This section also outlines the contributions and limitations of the proposed techniques.

3.1 Machine learning based techniques

ML is the art of making computers to perform actions autonomously, that is, without explicitly following pre-programmed instructions. ML evolved primarily from computer science and Artificial Intelligence, and also from other fields including applied mathematics, pattern recognition and computational learning theory (Buhmann 2015). ML algorithms are mostly used to handle problems involving automatic data classification (Bergholz et al. 2008). ML algorithms are capable of analyzing data and searching for hidden patterns in data (Ayodele 2010). Mannila (1996) explained that ML algorithms aims to predict patterns from data based on learned experiences. ML algorithms are divided into different classes, namely: supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning, transduction and learning to learn (Ayodele 2010). Most of the proposed credit card fraud detection techniques are based on supervised learning and few are based on semi-supervised learning. Some of these techniques are discussed next.

3.1.1 Hidden markov model

Khan et al. (2014a) proposed a technique based on HMM and K-clustering. In the study, authors used HMM to model a sequence of credit card transactions and used K-clustering algorithm to divide the transactions into three clusters: high, low and medium. Afterwards, incoming transactions were compared to past ten transactions performed by card user and authorized if there was a match. Otherwise, transaction will be terminated and IP address of the merchant to be defrauded will be traced using HMM. A notification will be sent to both the merchant system's administrator and mobile number of card owner. Authors noted that HMM was trained with Baum–Welch algorithm. Authors did not provide details about results obtained from the proposed solution.

Khan et al. (2013) proposed a solution to credit card fraud detection system based on HMM. The system performs detection using spending patterns of cardholders. During classification, system request for card information of user and compares the information to information stored

Table 1 Credit card fraud detection techniques

Technique category	Name of technique	References
Nature inspired	Artificial immune system	Wong et al. (2012), Soltani et al. (2012), Soltani Halvaiee and Akbari (2014)
	Genetic algorithm	Patel and Singh (2013), RamaKalyani and UmaDevi (2012)
Machine learning	NN	Modi et al. (2013), Van Vlasselaer et al. (2015)
	HMM	Mhamane and Lobo (2012a), Bhusari and Patil (2011), Mhamane and Lobo (2012b)
	Meta-learning	Stolfo et al. (1997), Sen and Dash (2013)
	SVM	Lu and Ju (2011)
	Frequent itemset mining	Seeja and Zareapoor (2014)
	Ontology	Potamitis (2013)
	Decision support system	Carminati et al. (2015)
	Modified fisher discriminant analysis	Mahmoudi and Duman (2015)
Hybridized—NI and ML	HMM and K-clustering	Khan et al. (2014a)
	ANN and simulated annealing	Khan et al. (2014b)
	Observation probability and HMM	Khan et al. (2013)
	Bayesian network and neural network	Maes et al. (2002)
	Decision tree and SVM	Sahin and Duman (2011)
	KNN + decision tree + naïve bayes	Pun (2011)
	ANN and logistic regression	Ganesh and Sena (2012)
	Recency-frequency-monetary and time-dependent score	Van Vlasselaer et al. (2015)
	Bagging and ensemble	Zareapoor and Shamsolmoali (2005)
	Transaction aggregation + logistic regression	Jha et al. (2012)

in a database. If there is a match, the system will request for PIN number of user. If the PIN is correct, and account balance is less than transaction amount, the system will ask user to provide answers to some secret questions. If the answers are correct, then an initial sequence of the users' 10 previous spending pattern will be extracted and passed to HMM for processing. Thereafter, HMM will calculate probability of acceptance for the new transaction. If the probability of acceptance revealed that there are no observed abnormalities, the transaction will be authorized. Else, if system observes some irregularities or if the number of transactions performed by user is less than 10 transactions, then user will be asked to provide answers to some security questions. If the answer provided is correct, the transaction will be performed in a secured mode; otherwise, the transaction will be terminated and referred back to the merchant's website. When a new transaction arrives, it is used to replace one of the old transactions in the sequence. Authors evaluated the performance of the proposed technique and it produced an accuracy of 92%.

Mhamane and Lobo (2012a) proposed a HMM-based fraud detection system. The system consists of 10 different modules. The first module allows users to interact with the system. In this module, users are allowed to login. The second module provides interaction between client and server. The third module allows a client to gain access to all items on the internet. The fourth module is responsible for authenticating transaction credentials entered by users. The module also generates a report if authentication is successful or not. The fifth module provides communication to servers via servlets. The sixth module is responsible for maintaining database of all account information of users. The seventh module maintains a database of past transactions already performed by users. The eighth module is responsible for performing classification of transaction. HMM is used to scan and classify transactions. The ninth module is for system administrators. It provides a Graphic User Interphase (GUI) that allows admin users to login and view account information of clients. New clients can also be added. The tenth module allows admin users to see accounts that are blocked. Admin users can also reactivate blocked account and change credentials of users. Authors did not report on result obtained from study.

Bhusari and Patil (2011) designed a fraud detection model based on Hidden Marcov Model (HMM) and K-clustering. Authors used HMM to monitor spending patterns of users. When a user initiates a payment request, firstly, it will be submitted to merchant's system for processing. If PIN entered by the user is correct, then transaction amount will be compared to account balance of card

holder. If the transaction amount is greater than the account balance, then the transaction will be denied and passed to a module responsible for fraud detection, otherwise, the transaction will be passed to the next stage for processing. Furthermore, with the aid of K-clustering algorithm, authors divided the amount of previous transactions (stored in the dataset) into three price ranges (low, medium and high). Moreover, HMM was used to check the last ten transactions (performed by card holder) for abnormalities in spending patterns. HMM use transition probabilistic calculation. If any abnormality is observed, user will be asked some security questions. If wrong answers are provided, the transaction will be denied and HMM will raise an alarm to the issuing bank. Authors noted that if the number of transactions performed by card holder is less than ten, then user will be asked some security questions. If provided answers are correct, user will be allowed to proceed with transaction. Some experiments were performed and it was reported that the proposed technique yielded an accuracy of 84% and a false alarm rate of 7%.

Mhamane and Lobo (2012b) proposed a HMM-based fraud detection technique. System architecture of the technique consist of the following component: legitimate user, fraudulent user, bank server and bank database. Bank database is used to store information about bank account holders. It is also used to store previous transactions of users. During training, system extracts sequence of transaction details about users from dataset and builds a HMM-based classification model using the extracted details. Furthermore, authors used trained model to classify incoming transactions. If there is a violation in the sequence of transactions, OTP will be sent to mobile number of user. Authors evaluated the performance of technique and it yielded a classification accuracy of 72%.

3.1.2 Support vector machines based techniques

Sahin and Duman (2011) performed a comparative study between SVM-based and decision tree based credit card fraud detection system. Authors used four kernels for SVM. During implementation, firstly, authors divided dataset used into three groups. In the first, second and third group, the ratio of fraudulent transaction to legitimate transaction was 1:1, 1:4 and 1:9 respectively. In each group, 70% of dataset was used for training and 30% of dataset was used for testing. Authors developed seven SVM-based and decision tree based models and tested each of them. Results from experiments revealed that decision tree based model outperformed SVM model. The models produced classification accuracy between the range of 83.02 and 94.76%.

Lu and Ju (2011) used PCA and Imbalanced Class Weight SVM (ICW-SVM) to develop a credit card fraud detection model. Authors used PCA for feature selection and used ICW-SVM for classification. Feature selection was achieved by calculating the principal components of all features and selecting features with the highest contribution rate. Selected features were then passed to ICW-SVM for classification. Authors noted that ICW-SVM handles data imbalance. Some experiments were performed and a classification accuracy of 91.28% was achieved. Furthermore, authors compared the result to result of three other algorithms: BN, C-SVM and Decision Tree (C5.0). ICW-SVM outperformed the three algorithms.

3.1.3 Meta-learning based techniques

Pun (2011) designed a credit card fraud detection model. Author's objective was to develop a classifier capable of filtering transactions for an existing Fraud detection system (called Falcon Fraud Manager) used by major banks in Canada. The model consists of three base classifiers, constructed using k-nearest neighbor, decision tree and naive Bayes algorithm respectively. Authors combined the output obtained from decision tree and K-CLUSTERING and passed it to naive Bayes for classification. Classification is divided into four stages. In the first stage, authors trained the base classifier on 50% fraudulent transactions and 50% legitimate transactions. Afterwards, authors tested the trained base classifier on a validation dataset and generated some predictions. In the third stage, authors combined the generated predictions with validation dataset and used the combined dataset to construct a naïve Bayes based meta-classifier. In the last stage, authors tested the base classifier obtained in the first stage and combined the result with the test dataset. Furthermore, authors used the combined dataset to re-train the meta-classifier. Result obtained from the re-trained meta-classifier is displayed as final output. Author performed some experiments to evaluate the performance of the designed meta-classifier and it yielded positive results. Additionally, authors compared the performance to performance of an existing bank's system, and it was reported that an improvement of 24–34% (resulting to a savings of $1.8 million to $2.6 million) was achieved.

Stolfo et al. (1997) proposed a meta-learning based fraud detection system. Aim of study is to develop a distributed fraud detection system for financial institutions in a network. The distributed system will enable financial institutions share fraudulent models in a secured manner. The shared model will be combined by a meta-learner into a single robust meta-classifier. The technique consists of two main components. The first component (called local fraud detection agents) consists of four classifiers: ID3, CART, BAYES and RIPPER. The second component (a meta-learning system) combines outputs obtained from the individual classifiers to make a decision. In the study,

authors developed different classification models using ID3, CART, RIPPER and Bayes. The models were trained and tested using different datasets, and outputs from the best N classifiers were combined by a meta-learner to generate a meta-classifier. Bayes, RIPPER, CART and ID3 yielded a False Positive (FP) rate of 13, 16, 16 and 23% respectively.

Sen and Dash (2013) investigated the performance of five meta learning algorithms in providing solution to credit card fraud detection. The algorithms include: Classification and Regression Tree (CART), Adaboost, Bagging, Logitboost and Grading. Result revealed that Bagging algorithm performed best (in terms of classification accuracy and misclassification rate) compared to the other four algorithms, while grading algorithm performed worst. Bagging, Logitboost, Adaboost, CART and grading produced a classification accuracy of 87.7, 85.5, 84.7, 83.4 and 53.6% respectively.

3.1.4 Frequent itemset mining

Seeja and Zareapoor (2014) proposed a fraud detection technique capable of handling transactions in an imbalanced dataset. Authors also proposed a matching algorithm for classification of incoming transactions. During training, authors extracted legal and fraudulent transaction pattern of all customers. Afterwards, authors used the extracted patterns to construct a classification model. During testing, if an incoming pattern matches more with a legal pattern, then the transaction will be classified as legitimate, otherwise, it will be classified as illegal. Authors constructed two patterns for each customer—a fraud and legitimate pattern. Furthermore, authors applied frequent itemset mining on transactions extracted from dataset. Frequent itemset mining evaluates transactions and returns different group of attributes. The group with the largest number of attributes is said to be the customer's legal pattern. During classification, customer's details are extracted from database. Afterwards, legal and fraud transactions for each customer are separated. Furthermore, frequent itemset mining algorithm is applied to legal transactions of each customer, and the algorithm returns a set containing different group of attributes. Thereafter, the group with highest number of attributes are selected and stored in a database. Furthermore, frequent itemset mining algorithm is applied to fraud transactions of each customer and the algorithm returns a set containing different group of attributes. Thereafter, the group with the highest number of attributes are selected and stored in a database. Furthermore, for an incoming transaction, a matching algorithm is used scan the legal and fraud database. If an incoming pattern matches more with legal pattern, then algorithm will classify the transaction as legitimate, otherwise, the algorithm will classify the transaction as illegal. Authors performed some experiments and compared its performance to four other classifiers: SVM, RF, NB and KNN. Result revealed that the proposed technique yielded the best fraud detection rate.

3.1.5 Transaction aggregation

Jha et al. (2012) proposed a credit card fraud detection technique based on transaction aggregation. Authors combined fraud and legitimate transactions of different time periods. Afterwards, authors used aggregated transactions to create variables, which were in turn used to train a logistic regression model. Authors performed series of experiments and a classification accuracy of 99% was achieved.

3.1.6 Ensemble based technique

Zareapoor and Shamsolmoali (2005) proposed a credit card fraud detection model based on bagging ensemble classifier. The primary objective of study was to compare the performance of SVM, NB and KNN to bagging ensemble classifier based on decision tree. Authors evaluated the performance of SVM, NB and KNN. Moreover, authors compared the result obtained to bagging ensemble classifier. Results revealed that bagging ensemble classifier yielded better fraud catching rate and false alarm rate. Result also revealed that bagging ensemble classifier is capable of handling data imbalance.

3.1.7 Ontology-based technique

Potamitis (2013) in a master's thesis, designed an ontology-based expert system for conceptualizing characteristics of existing fraud detection techniques and characteristics of fraud attacks. Specifically, authors designed the expert system to handle credit card fraud, bankruptcy fraud, credit card application fraud and 25 detection techniques. To achieve this, authors first identified different fraud detection techniques from literature. Furthermore, authors analyzed the characteristics of the identified techniques and conceptualized the information into mathematical representations. Afterwards, authors used the mathematical representations to build the ontology knowledge base system. Moreover, authors used the knowledge based system to design an expert system. Authors noted that the expert system can assist software developers to choose techniques to implement for specific kind of fraud. Authors performed different tests on the expert system and it yielded excellent results.

3.1.8 Decision support system

Carminati et al. (2015) developed an online fraud detection system called BANKSEALER. The system is based on a

combination of semi-supervised and unsupervised technique. It builds models for different customer behavior based on transactions stored in a database. During classification, BANKSEALER first weighs anomaly of each user transaction and then search for other users with comparable spending patterns. Lastly, the system measures the abnormality of current spending pattern of user relating to past spending pattern of user. BANKSEALER is currently deployed as a pilot project in a renowned Italian bank.

3.1.9 Modified fisher discriminant analysis based technique

Mahmoudi and Duman (2015) proposed a novel credit card fraud detection technique based on Fisher Discriminant Function. Authors developed a modified version of the function. The modified version contains a weight function responsible for classifying transactions with higher financial cost implication. Authors developed five weight functions. The weight function compares available limit on a card to average limits on other cards, and assigns higher weights to cards with higher limit. Authors used decision tree for feature selection. Authors evaluated the performance of the proposed technique and it yielded positive results.

3.2 Nature inspired based techniques

NI techniques refers to techniques inspired by nature's problem solving ability (Rozenberg et al. 2011). Nature is the source of inspiration to NI algorithms (Batouche and Meshoul 2010). For example, Ant Colony Optimization is inspired by the methods used by ants to seek for pathways between their colony and a food source (Dorigo 1992) and Genetic Algorithm is inspired by the process of natural selection (Mitchell 1998). NI algorithms are designed to handle complex real world classification and optimization related problems, such as timetabling problem (Cerdeira-Pena et al. 2008), travelling salesman problems (Applegate et al. 2006) and hostel allocation problems (Adewumi and Ali 2010). Generally, NI algorithms are used to search vast solution spaces for optimal results within a reduced time period. Some NI-based techniques used to provide solution to credit card fraud detection are discussed next.

3.2.1 Artificial immune system based techniques

Wong et al. (2012) proposed an AIS-based credit card fraud detection technique. The AIS system consist of six components: user interface, detector set, transaction processor, detector generator, database and automated testing machine. The user interface is responsible for accepting inputs (in form of transactions). It is also be used to check system status. The automated testing engine is responsible for sending transactions to system from a pool of transactions stored in a database. It is also used to save statistics-related data about system's performance in the database. Detector generator is used to produce mature detectors (using negative selection) and memory detectors. It is also used for evolution of memory detector. Transaction processor is used to process and classify transactions. During implementation, authors extracted data from dataset and mapped them into a bit pattern using a matching algorithm. Afterwards, authors used the matching algorithm to classify transactions. The AIS system consist of the following: a representation and matching algorithm, negative selection algorithm, vaccination algorithm and an algorithm for memory cell evolution. Representation and matching algorithm was used to classify transactions, vaccination algorithm was used to reinforce the system's learning ability to adapt to evolving patterns. Negative selection algorithm was used to generate mature detectors—which were used to classify transactions. Matching algorithm consist of rules created for different transactions extracted from database. During classification, output for each rule was combined and mutated. Authors designed the mutation function using Genetic Algorithm. Furthermore, the mutated rules were compared to incoming transactions. If there was no match the rules were destroyed and new set of rules were created. Otherwise, the rules was passed through negative selection process to ensure that they are self-tolerant. If they are self-tolerant, then they are kept, otherwise, they are destroyed and new set of rules are generated. Authors tested the performance of the proposed technique and it produced a classification accuracy of 71.3%.

Soltani et al. (2012) proposed an AIS-based fraud detection algorithm. Algorithm used clonal selection to create detectors. In the study, authors generated fraud and normal detectors for all classes and used KNN algorithm for classification. Furthermore, authors calculated Euclidean distance for all records in the database and selected records with the lowest distance as the k neighbors. Authors performed some experiments and promising result was achieved.

Soltani Halvaiee and Akbari (2014) proposed an improved credit card fraud detection model based on AIS. During memory cell generation, distance between each training records and their corresponding ARB (Artificial Recognition Ball) is calculated. Afterwards, records with low distance are selected for mutation. If the selected records belong to same class, it is selected for mutation. Otherwise, records with large distances, in the same class are selected. At the end of memory cell generation, each cell is ranked based on its distance between each record it matches. If a memory cells performs wrong classification, it will be rated based on its distance between the wrongly

classified records. Rating is performed using KNN algorithm. Authors explained that rank will be positive if memory cell and matched records belong to the same class, otherwise, rank will be negative. Authors tested the model and it yielded a detection rate and FP rate of 0.518 and 0.017 respectively.

3.2.2 Genetic algorithm based techniques

Patel and Singh (2013) proposed a GA-based credit card fraud detection system with the aim of reducing the amount of credit accessible to fraudsters. Authors defined an objective function with variable misclassification cost. The objective function aims at reducing the number of transactions with high classification cost. During classification, authors extracted credit card transactions from dataset and stored them in a database. Afterwards, authors calculated critical values for each transaction. Authors also extracted the following from each transaction: frequency count for credit card usage, credit card overdraft, location where the credit card was used, balance on account linked to credit card, average spending pattern of the credit card owner. Furthermore, authors used Genetic Algorithm (GA) to generate new critical values. Finally, the new critical values were then used for classification. Authors did not report results obtained from study.

Duman and Ozcelik (2011) introduced a hybridized credit card fraud detection system capable of handling misclassification cost. GA and Scatter Search (SS) algorithms were combined and used to build a robust credit card fraud detection algorithm called GASS. Authors worked with 43 parameters and a population size of 50. Forty-seven of the 50 solutions were determined by generating 47 random numbers for 43 parameters. The remaining 3 solutions were solutions for generating maximum number of alerts (MAX), minimum number of alerts (MIN) and solution used for production (PRD). In the reproduction stage, authors combined parameter values of two parent solutions to obtain a child solution. Authors noted that the reproduction process is different from the reproduction process of GA but similar to scatter search algorithm. Authors also noted that the classification steps of GASS is similar to standard GA, but with some element of SS algorithm. Authors carried out several experiments to evaluate the performance of the proposed technique, and results showed that GASS algorithm improved the performance of an existing fraud detection system by 200%.

RamaKalyani and UmaDevi (2012) proposed a GA-based credit card fraud detection technique with varied misclassification cost. The objective of study was to limit the total amount of credit accessible by fraudsters. During classification, authors extracted the following information from dataset: frequency of credit card usage, the location of usage the credit card overdraft, the available balance in the credit card and the average amount spent per day. Afterwards, authors used GA to generate critical values and also generate fraud transactions. Thereafter, new transactions are compared to the generated critical values and classified accordingly. Authors repeated the process until a user-defined threshold was reached. Authors tested the performance of technique and it yielded positive result.

3.2.3 Artificial neural network based techniques

Khan et al. (2014b) used simulated annealing and NN to develop a credit card fraud detection technique. Authors used simulated annealing to control parameters in the NN. Authors generated a random weight for all connections in the NN, and normalized them using TANH activation function. Afterwards, authors created a weight matrix and randomized the matrix using simulated annealing. Furthermore, authors generated new weights from output obtained from previous circle. Furthermore, authors compared the weights to previous weights and update them if there is an improvement. Authors also reduced the temperature after each iteration and compared it to a user-defined temperature. If the temperature is lower, the process will be repeated again. Authors evaluated the performance of technique and it yielded a classification accuracy of 89.6%.

Maes et al. (2002) performed a comparative study between ANN and Bayesian Network for credit card fraud detection. In the study, authors extracted features from dataset, pre-processed and normalized them. Afterwards, authors used the features to construct a Bayesian Network and ANN-based models. Also, authors used STAGE algorithm to select the optimal configuration for ANN. Authors conducted different experiments, and result revealed that BN outperformed ANN in both classification speed and accuracy. However, authors pointed out that fraud detection process of ANNs is faster.

Modi et al. (2013) constructed a NN rule-based fraud detection system capable of providing solution to credit card fraud. Authors used single layer feed forward NN algorithm. In the study, authors divided fraudulent transactions into four groups, namely: low, high, risky and high risk. Transactions are classified based on defined rules. If a processed transaction is fraudulent, it will be assigned to any of the four groups. Authors evaluated the performance of the algorithm. However, much detail about the results was not reported.

Ganesh and Sena (2012) developed a credit card fraud detection model based on ANN and logistic regression. Authors considered a classification problem with variable misclassification cost. Also, authors used GA to optimize classifier parameters. During classification, authors

identified spending pattern of cardholder, computed some set of probability and constructed some sequence. Finally, authors used the sequence to construct a NN-based and logistic regression based model.

Van Vlasselaer et al. (2015) proposed a novel credit card fraud detection technique called APATE. The technique combined two features. First feature is based on characteristics of incoming transactions and spending history of customers. Authors used Recency-Frequency-Monetary (RCF) fundamentals to derive this feature. The second feature is a time-dependent score based on network used by card holders and merchants. Incoming transactions are classified based on the following features: average number of past transactions over a time period, average time interval between incoming and previous transaction, the value of the transaction. Incoming transactions are also classified based on a score indicating merchants frequently linked to fraud. Incoming transactions are also classified based on credit card holders with stolen cards or card holders that seldom perform transactions. Authors combined all the features and designed 78 variables which were used to construct three classification models based on logistic regression, random forest and NN. Authors performed some experiments and reported that an AUC score higher than 0.98 was obtained. RF, NN and logistic regression yielded a classification accuracy of 98.7, 93.84 and 95.92% respectively.

3.3 Survey summary

The surveyed techniques reveal that various ML and NI algorithms have been used to handle credit card fraud detection. As shown in Fig. 2, HMM, NN, SVM, AIS and GA are the most popularly used techniques in the domain of credit card fraud detection. Furthermore, among these widely used algorithms, as shown in Figs. 2 and 3, HMM and NN has gained more attention and they have been used consistently for the past 4 years. These algorithms are used alone or in combination with other techniques, such as meta-learning or ensemble techniques. HMM is simple to implement, it removes classification complexity and it can be used to produce simple classification models (Khan et al. 2013; Bhusari and Patil 2011). The training time of ANN takes several hours (Maes et al. 2002), sometimes days (Khan et al. 2014b). NN-based algorithms requires parameter tuning algorithm (such as GA) and an effective algorithm for good network configuration (Khan et al. 2014b). Furthermore, some authors used Meta-classifiers, which yielded good results (Pun 2011; Stolfo et al. 1997), however their classification speed is slow because they involve combination of several classifier. Moreover, fisher discriminant analysis is one technique that has not been fully explored in the domain of credit card fraud detection.

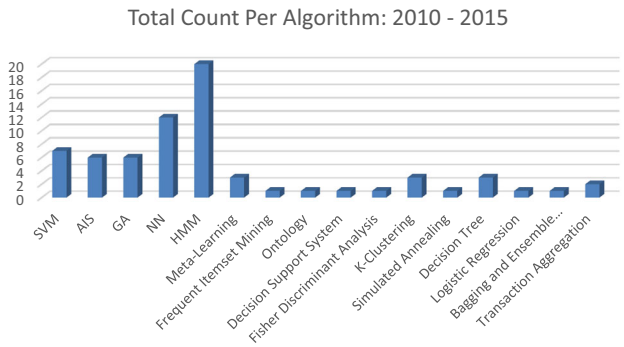

Fig. 2 Total number of proposed techniques for each algorithm between years 2010 and 2015

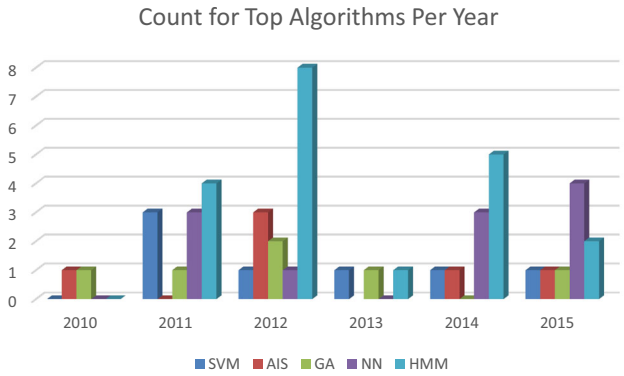

Fig. 3 Number of proposed techniques for top six algorithms per year

Technique proposed by Mahmoudi and Duman (2015) is one of the few techniques that is based on fisher discriminant analysis. The technique was designed to maximize high value transactions and FNs. Experiments performed in the study yielded good results, implying that fisher discriminant analysis is a promising algorithm to explore. Another area that has not been explored is ontology-based technique. Potamitis (2013) is one of the few that ontology-based technique. The author introduced an ontology-based expert system for conceptualizing characteristics of existing fraud detection techniques. However, the technique is static thus requiring regular update of knowledge base.

As mentioned above, NI techniques has been used to provide solution to credit card fraud detection problems. NI techniques are capable of improving classification speed and accuracy of ML algorithms. Authors in Wong et al. (2012), Soltani et al. (2012), and (Soltani Halvaiee and Akbari (2014) proposed AIS-based credit fraud detection techniques. AIS-based systems aims to model a representation of detector and antigen relationship (Wong et al. 2012). Afterwards, a matching algorithm is required to determine the strength of affinity between the antigen and detector. However, unlike AIS, matching algorithms are

not capable of detecting non-self organisms (Wong et al. 2012). AIS is commonly used to model negative selection (Wong et al. 2012). Wong et al. (2012) noted that AIS-based techniques are not dynamic. Authors handled this limitation by designing a dynamic AIS-based system that models fraudulent patterns in ecommerce systems. Also, Soltani Halvaiee and Akbari (2014) introduced an improved credit card fraud detection model with a modified method for performing negative selection. However, memory generation phase and calculation of affinity are time-consuming. Additionally, Soltani et al. (2012) proposed a novel credit card fraud detection model capable of handling misuse and anomaly detection. However, FP of the model is too high and generating detectors for all transactions can affect the classification speed.

As above-mentioned, GA is one of the popular NI algorithms that have been used to handle credit card fraud. Authors in Patel and Singh (2013), RamaKalyani and UmaDevi (2012) used GA to improve credit card fraud detection. Patel and Singh (2013) used GA to generate nodes and hidden layer for NN. Duman and Ozcelik (2011) used GA in combination with scatter search to design a fraud detection technique with new classification cost function. Authors in RamaKalyani and UmaDevi (2012) and Ganesh and Sena (2012) used GA for parameter tuning. However, experiments performed by Duman and Ozcelik (2011) revealed that GA's convergence rate is slow, especially, when applied to large datasets. Furthermore, authors in Duman and Ozcelik (2011), Patel and Singh (2013) and RamaKalyani and UmaDevi (2012) proposed techniques for handling misclassification cost. Duman and Ozcelik (2011) noted that data mining algorithms cannot effectively handle classifications with misclassification costs. Additionally, although, high value transactions has more impact, low value transactions should not be underestimated. This is because, a system can be compromised if multiple low value transactions are performed.

Moreover, many ML techniques has been used to handle credit card fraud. Authors in Khan et al. (2013, 2014a), Mhamane and Lobo (2012a), Bhusari and Patil (2011) and Mhamane and Lobo (2012b) used HMM. Khan et al. (2014a) used HMM in combination with K-clustering. Authors used HMM to model sequence of credit card transactions. Authors trained HMM with Baum–Welch algorithm. Additionally, Mhamane and Lobo (2012b) proposed a ML-based technique for handling internet banking transactions. Authors used One Time Password (OTP) as an additional security feature. ANN and BNN are two other ML techniques that has been explored in literature. As mentioned above, NN-based techniques are generally slow. Maes et al. (2002) performed a comparative study between BNN-based and ANN-based credit card fraud detection techniques and results revealed that BNN has higher classification speed compared to ANN. Authors suggested that ANN can be improved by removing connections and perceptron that are not used in training and performing weight updates. Radial basis networks and SVMs are good algorithms that can be used for weight updates (Maes et al. 2002). ANN also requires effective algorithms for performing parameter selection (Maes et al. 2002; Khan et al. 2014b). SVM is another ML algorithm that has been used to solve credit card fraud detection. The performance of SVM improves as the number of data size increases (Sahin and Duman 2011). Lu and Ju (2011) designed a SVM-based technique capable of handling classification that requires assigning variable weights to different classes. Authors noted that adjusting class weights can improve the classification speed and accuracy of a classifier.

Decision trees is one of the ML algorithms that has not been fully explored in the domain of credit card fraud. One of the few authors that have used decision tree is Sahin and Duman (2011). Authors performed a comparative study between SVM-based and decision trees based credit card fraud detection systems, and result revealed that decision tree outperformed SVM. Meta-learning technique is another approach that have been used to tackle credit card fraud. Pun (2011) proposed a technique based on meta-classifier model consisting of three classifiers: KNN, decision tree and Bayesian algorithm. Authors noted that the technique was deployed in series with an existing bank's system and it yielded an improvement of between 28 and 34% performance. Stolfo et al. (1997) also proposed a meta-learning technique. The technique consist of two main component. The first component (called local fraud detection agents) consist of four classifiers: ID3, CART, BAYES and RIPPER. The second component is a meta-learning system that combines the outputs obtained from the individual classifiers to make a decision. Results obtained from many of the proposed meta-classifier models are good, however, as mentioned above, classification speed of meta-classifiers is slow because, it involves combination of outputs from two or more classifiers. Also, experiments performed by Stolfo et al. (1997) revealed that TP and FP rate of meta-classifiers increases as labelled fraud data samples increases. Also, experiment revealed that a balanced dataset will yield an improved classification accuracy (Stolfo et al. 1997). Additionally, experiment revealed that the best meta-classifier is BAYES (Stolfo et al. 1997).

Most of the existing studies focused on classification of customer spending profile analysis and derived attributes (Seeja and Zareapoor 2014). However, few studies focused on classification of anonymous dataset. One of the few authors that worked on this is Seeja and Zareapoor (2014).

Authors proposed a credit card detection technique capable of handling transactions in an imbalanced and anonymous dataset. The technique has good and balanced classification rate, however, fraudulent and legal patterns formed for customers and stored in a database requires regular updates. Furthermore, authors noted that proposed technique cannot detect transactions with similar fraud and legal patterns. Another unique technique proposed in literature is Jha et al. (2012). Authors proposed a technique based on aggregation of transactions. In the study, authors combined legal and fraudulent transactions and used the combined dataset to construct a classifier. Authors explained that both patterns were combined to capture the difference between buying behavior of customers. Authors also noted that fraud detection involving large dataset requires dataset grouping and creating new attributes. In another work, Van Vlasselaer et al. (2015) introduced a technique that combines two group of features. The first group of features (called intrinsic features) were obtained from incoming transactions and spending history of customers. Authors used Recency-Frequency-Monetary (RFM) fundamentals to obtain this group of features. The second group of features were obtained by calculating a time-dependent score based on the network of credit card holders and credit card merchants. Authors used NN, logistic regression and RF to test model and RF yielded the best result.

Summarily, most of the proposed techniques yielded promising results. However, most of the datasets used are very imbalanced. Most dataset contained higher percentage of legal transactions compared to fraudulent transactions. Furthermore, most of the proposed techniques were not tested on real-world dataset; they were tested on artificially generated dataset. This is because, most financial institutions do not release dataset due to confidentiality agreement they signed with their customers. Additionally, classification speed and accuracy of most of the techniques is low. Most authors did not explore the use of NI techniques.

3.4 General comments on reviewed techniques

Outlined below and in Table 2 are the summarized limitation of the credit card fraud detection techniques reviewed in this study. Furthermore, Table 2 shows the contributions of all techniques reviewed in this paper.

(a) One of the major challenges in credit card fraud detection is lack of good dataset for experimentation. Most of the available data are imbalanced. They contain more of legitimate transactions and very few fraudulent transactions. This data imbalance has made fraud detection a challenging task to tackle (Duman and Ozcelik 2011). Lack of dataset is primarily because of privacy and confidentiality issues arising from financial transactions.

(b) Many of the reviewed techniques are not capable of handling transactions with variable misclassification costs. ML algorithms are not designed to handle variable misclassification cost; their main objective is to minimize the number of incorrectly classified data instances (Duman and Ozcelik 2011). Duman and Ozcelik (2011) noted that credit card fraud detection system should aim at minimizing fraud with higher misclassification cost.

(c) Many of the proposed techniques yielded low classification accuracy. This can be attributed to the fact that they did not explore NI-based feature selection or parameter selection techniques, as revealed in Table 1.

(d) Researchers seldom provide full details of their work (results, features used, etc.) making it difficult to benchmark results of newly designed techniques.

(e) Training time of ANN takes several hours, sometime days (Maes et al. 2002).

(f) Classification speed of meta-classifiers is slow, because, they involve the combination of various classifiers. Also, Stolfo et al. (1997) TP and FP rate of meta-classifiers increases as labelled fraud data samples increases.

(g) AIS-based techniques are not dynamic. Also, memory generation phase and calculation of affinity are time-consuming (Wong et al. 2012).

(h) GA takes very long to converge when applied to large datasets (Duman and Ozcelik 2011).

(i) Data mining algorithms cannot effectively handle classifications with misclassification costs (Duman and Ozcelik 2011).

(j) Some of the proposed techniques cannot detect transactions with similar fraud and legal patterns.

(k) Due to lack of dataset availability, some authors used artificially generated data, which affect system performance.

4 Conclusion and recommendations

Credit card detection is a fascinating domain. However, as shown in Fig. 4, it has not been fully harnessed as not there are still rooms for further research in this area. Few authors that have worked in this domain provided little or no details on dataset used, features used and results obtained in their studies, making it very difficult to develop new techniques. Furthermore, many authors made use of imbalanced dataset. Additionally, many of the credit card detection techniques

Table 2 Contributions and limitations of reviewed techniques

Author	Contribution(s)	Limitation(s)	Result
Wong et al. (2012)	An improved AIS-based credit card detection technique was proposed	Classification accuracy is low	Detection rate of 71.3% was achieved
Patel and Dheeraj (2013)	Result not reported	Low impact transactions was not properly considered. Multiple low impact transactions can compromise the system	Result not reported
Khan et al. (2014a)	Result not reported		Result not reported
Khan et al. (2014b)	Real time fraud detection technique was introduced	Misclassification rate is low Low classification speed Dataset size is low Training time is long	CA: 89.6%
Khan et al. (2013)	A HMM-based credit card fraud detection technique was introduced	CA is low	CA: 92%
Maes et al. (2002)	ANN-based and BN-based technique was proposed	Proposed ANN technique can only handle discrete variables	ANN FP rate: 70%, BN FP rate: 74%
Sahin and Duman (2011)	A credit card fraud detection technique based on SVM and decision tree was proposed	Data imbalance	CA between 83.02% and 94.76%
Duman and Ozcelik (2011)	A novel classification cost function for fraud detection related problems was introduced	Dataset size used for training is small Data imbalance is high	Proposed algorithm improved classification by 200%
Modi et al. (2013)	New and improved credit card fraud detection solution was proposed	ANN training time is slow	Result reported was not clear
Mhamane and Lobo (2012a)	Details about result was not reported	Details about result is not reported	Result obtained from the study is not reported
RamaKalyani and UmaDevi (2012)	Result reported is not comprehensive	Result reported is not comprehensive	Result reported is not comprehensive
Pun (2011)	An improved credit card detection model was introduced Proposed technique performed better than an existing bank's technique	Proposed model is slow, it consists of three classifiers	An improvement of 24–34% was achieved
Stolfo et al. (1997)	A technique based on meta-learning was proposed	Classification speed is slow, it consist of a combination of several classifiers	FP rate of 13, 16, 16 and 23% was achieved
Sen and Dash (2013)	Results revealed that Bagging is a good meta classifier and grading is not a good meta classifier for credit card fraud		CA for Bagging: 87.7% CA for Logitboost: 85.5% CA for Adaboost: 84.7% CA for CART: 83.4% CA for grading: 53.6%
Lu and Ju (2011)	Proposed technique is capable of handling data imbalance	CA is low. Dataset is highly imbalanced	CA: 91.28%
Bhusari and Patil (2011)	HMM-based model was proposed	CA is low	CA: 84%
Mhamane and Lobo (2012b)	New authentication technique was introduced	CA is low	CA: 72%
Seeja and Zareapoor (2014)	An improved and robust model capable of handling data imbalance was introduced. System was tested on large number of data instance	Proposed technique cannot detect transactions with similar fraud and legal patterns Proposed technique is not dynamic. It has low classification speed	Detection rate is improved by 23% Cost is decreased by 85% Training time is reduced by 40%
Jha et al. (2012)	Novel model based on transaction aggregation was proposed	Time stamp of transactions is not present in dataset	CA: 99%

Table 2 continued

Author	Contribution(s)	Limitation(s)	Result
Van Vlasselaer et al. (2015)	A novel, dynamic and accurate model was introduced New features was also introduced	Data imbalance is too high	AUC score higher than 0.98 was obtained. CA for RF: 98.7% CA for NN: 93.84% CA for logistic regression: 95.92%
Mahmoudi and Duman (2015)	A novel technique based on modified version of Fisher Discriminant Function was proposed	Proposed technique cannot effectively handle false negatives	Proposed technique outperformed ANN, decision tree, NB and Normal Fisher
Soltani et al. (2012)	A novel model capable of handling misuse and anomaly detection was proposed	FP is too high Classification speed can be affected by generating detectors for all transactions	Detection Rate: 100% FP rate: 13%
Soltani Halvaiee and Akbari (2014)	A modified method for negative selection was introduced	Memory generation phase and calculation of affinity are time-consuming	Detection rate: 51.8% FP rate: 0.017
Zareapoor and Shamsolmoali (2005)	A novel technique based on bagging ensemble classifier was introduced	Bagging ensemble classifier involves classification of different datasets, hence it is slow	Fraud alarm rate: 90% false alarm rate: 0.02%
Potamitis (2013)	An ontology-based expert system for fraud detection was proposed	Proposed expert system is static, it requires regular updates	CA: 100%
Carminati et al. (2015)	A semi-supervised and unsupervised decision support system for handling fraud and anomaly detection was proposed	Clustering phase of proposed technique consume large storage space Synthetically generated data was used to build model	Detection rate: 98%

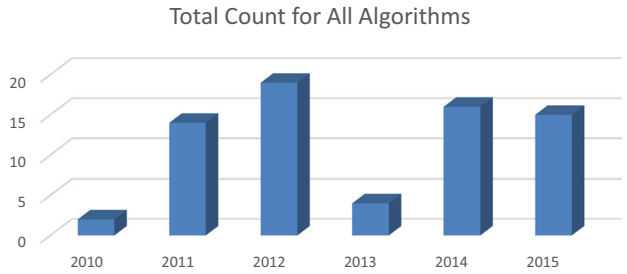

Fig. 4 Total number of proposed techniques between years 2010 and 2015

surveyed in this paper used ML algorithms. However, many of them yielded low classification accuracy, FP rates and False Negative rates. This likely because, the techniques were not combined with good and effective feature selection and parameter optimization technique. NI algorithms can be used to improve the classification speed and accuracy of credit card fraud detection system. Future work should focus on designing classification models capable of handling variables with different misclassification cost. Also, future work should consider focusing on constructing accurate classification models based on NI-techniques. This will likely increase the performance of credit card detection solutions. Other observations cum recommendations include:

(a) Researchers need to focus on developing algorithms that can handle classification tasks with variable misclassification cost.
(b) Some authors used falsely generated data. There is need for researcher to provide more details on methodology and result. This will enable new researchers to develop better and more robust credit card detection system.
(c) Credit card fraud detection systems usually process millions of transactions. Hence, to improve the classification performance of fraud detection systems, there is a need for robust data dimension reduction technique and feature selection technique. NI-techniques are good candidates for this task.
(d) System developers can consider using HMM as it is simple to implement. In addition, it removes classification complexity and can be used to produce simple classification models (Khan et al. 2013; Bhusari and Patil 2011).
(e) NN-based algorithms require both parameter tuning and an effective network configuration algorithms (Khan et al. 2014b). GA has been recommended in literature for parameter tuning (Khan et al. 2014b).
(f) Experiments performed by Stolfo et al. (1997) revealed that TP and FP rate of meta-classifiers increases as labelled fraud data samples increases.

The experiment revealed that a balanced dataset will yield an improved classification accuracy.

(g) Misclassification cost should be handled with care. Although, high value transactions has more impact, low value transactions should not be underestimated. This is because a system can be compromised if multiple low value transactions are done.

(h) Adjusting class weights can improve the classification speed and accuracy of a classifier (Lu and Ju 2011).

References

Adewumi AO, Ali MM (2010) A multi-level genetic algorithm for a multi-stage space allocation problem. Math Comput Model 51:109–126

Applegate DL, Bixby RE, Chvátal V, Cook WJ (2006) The Traveling Salesman Problem: A Computational Study. Princeton University Press, New Jersey. ISBN: 9780691129938

Ayodele TO (2010) Types of machine learning algorithms. In: Yagang Zhang (ed) New Advances in Machine Learning. In-Tech Publisher, pp 19-48. ISBN: 978-953-307-034-6

Batouche M, Meshoul S (2010) Nature Inspired intelligent techniques for problem solving. Technical Report, King Saud University, Riyadh, Kingdom of Saudi Arabia

Bergholz A, Chang JH, Paaß G, Reichartz F, Strobel S (2008) Improved phishing detection using model-based features. In: Proceedings of the conference on email and anti-spam (CEAS), Mountain View, CA, USA

Bhusari V, Patil S (2011) Study of hidden markov model in credit card fraudulent detection. Int J Comput Appl 0975–8887(20):33–36

Buhmann JM (2015) Machine learning. https://ml2.inf.ethz.ch/courses/ml/. Accessed 08 Dec 2015

Carminati M, Caron R, Maggi F, Epifani I, Zanero S (2015) BankSealer: a decision support system for online banking fraud analysis and investigation. Comput Secur 53:175–186

Cerdeira-Pena A, Carpente L, Farina A, Seco D (2008) New approaches for the school timetabling problem. In: Seventh Mexican international conference on artificial intelligence (MICAI'08). Atizapan de Zaragoza, pp 261–267

Dorigo M (1992) Optimization, learning and natural algorithms. Ph. D. thesis, Politecnico di Milano, Italy

Duman E, Ozcelik MH (2011) Detecting credit card fraud by genetic algorithm and scatter search. Exp Syst Appl 38:13057–13063

Ehramikar S (2000) The enhancemeat of credit card fraud detectioa systems using machine learning methodology. Masters, University of Toronto, Canada

FFA (2015) Stop and spot: cardnot-present fraud. http://www.financialfraudaction.org.uk/. Accessed 02 Dec 2015

Gadi MFA, do Lago AP, Wang X (2016) A comparison of classification methods applyed on credit card fraud detection. Technical Report, Sao Paulo, Brazil

Ganesh K, Sena PV (2012) Novel artificial neural networks and logistic approach for detecting credit card deceit. Int J Comput Sci Netw Secur 13:58–65

Insider B (2015) Payments companies are trying to fix the massive credit-card fraud problem with these 5 new security protocols. http://www.businessinsider.com/how-payment-companies-are-trying-to-close-the-massive-hole-in-credit-card-security-2015-3. Accessed 01 Dec 2015

Jha S, Guillen M, Westland JC (2012) Employing transaction aggregation strategy to detect credit card fraud. Exp Syst Appl 39:12650–12657

Khan AP, Mahajan VS, Shaikh SH, Koli AB (2013) Credit card fraud detection system through observation probability using hidden markov model. Int J Thesis Proj Diss 1:7–16

Khan MZ, Pathan JD, Ahmed AHE (2014a) Credit card fraud detection system using hidden markov model and K-clustering. Int J Adv Res Comput Commun Eng 3:5458–5461

Khan AUS, Akhtar N, Qureshi MN (2014b) Real-time credit-card fraud detection using artificial neural network tuned by simulated annealing algorithm. In: Conference on recent trends in information, telecommunication and computing, ITC, pp 113–121

Lu Q, Ju C (2011) Research on credit card fraud detection model based on class weighted support vector machine. J Converg Inf Technol 6:62–68

Maes S, Tuyls K, Vanschoenwinkel B, Manderick B (2002) Credit card fraud detection using Bayesian and neural networks. In: Proceedings of the 1st international naiso congress on neuro fuzzy technologies, pp 261–270

Mahmoudi N, Duman E (2015) Detecting credit card fraud by modified fisher discriminant analysis. Exp Syst Appl 42:2510–2516

Mannila H (1996) Data mining: machine learning, statistics, and databases. In: Proceedings of the 8th international conference on scientific and statistical database management, Washington, DC, USA, pp 2–9

Mhamane S, Lobo L (2012a) Fraud detection in online banking using HMM. In: International conference on information and network technology (ICINT 2012), Singapore, pp 200–204

Mhamane SS, Lobo LJ (2012b) Use of hidden markov model as internet banking fraud detection. Int J Comput Appl 45:5–10

Mitchell M (1998) An introduction to genetic algorithms. MIT Press, New York

Modi H, Lakhani S, Patel N, Patel V (2013) Fraud detection in credit card system using web mining. Int J Innov Res Comput Commun Eng 1:175–179

Patel RD, Singh DK (2013) Credit card fraud detection & prevention of fraud using genetic algorithm. Int J Soft Comput Eng 2:2231–2307

Patidar R, Sharma L (2011) Credit card fraud detection using neural network. Int J Soft Comput Eng 1:2231–2307

Potamitis G (2013) Design and implementation of a fraud detection expert system using ontology-based techniques. Master Thesis, University of Manchester, UK

Quah JT, Sriganesh M (2008) Real-time credit card fraud detection using computational intelligence. Exp Syst Appl 35:1721–1732

RamaKalyani K, UmaDevi D (2012) Fraud detection of credit card payment system by genetic algorithm. Int J Sci Eng Res 3:1–6

Rozenberg G, Bck T, Kok JN (2011) Handbook of natural computing. Springer Publishing Company, Incorporated, Berlin

Sahin Y, Duman E (2011) Detecting credit card fraud by decision trees and support vector machines. In: Proceedings of the international multiConference of engineers and computer scientists (IMECS 2011), vol 1, Hong Kong, pp 1–6

Seeja K, Zareapoor M (2014) FraudMiner: a novel credit card fraud detection model based on frequent itemset mining. Sci World J 2014:10

Sen SK, Dash S (2013) Meta learning algorithms for credit card fraud detection. Meta 6:16–20

Soltani Halvaiee N, Akbari MK (2014) A novel model for credit card fraud detection using Artificial Immune Systems. Appl Soft Comput 24:40–49

Soltani N, Akbari MK, Javan MS (2012) A new user-based model for credit card fraud detection based on artificial immune system. In: 2012 16th CSI international symposium on artificial intelligence and signal processing (AISP), Shiraz, Fars, pp 029–033

Stolfo S, Fan W, Lee W, Prodromidis A, Chan P (1997) Credit card fraud detection using meta-learning: Issues and initial results. AAAI Workshop on AI approaches to fraud detection and risk management, pp 83–90

Van Vlasselaer V, Bravo C, Caelen O, Eliassi-Rad T, Akoglu L, Snoeck M et al (2015) APATE: a novel approach for automated credit card transaction fraud detection using network-based extensions. Decis Support Syst 75:38–48

VISA (2005a) Fact sheet 12: security and fraud prevention. http://www.visa-asia.com/ap/au/mediacenter/factsheets/includes/uploads/FS12_security_amd_prevention.pdf. Accessed 02 Dec 2015

Wong N, Ray P, Stephens G, Lewis L (2012) Artificial immune systems for the detection of credit card fraud: an architecture, prototype and preliminary results. Inf Syst J 22:53–76

Pun JK-F (2011) Improving credit card fraud detection using a meta-learning strategy. Master Thesis, University of Toronto, Canada

Zareapoor M, Shamsolmoali P (2005) Application of credit card fraud detection: based on bagging ensemble classifier. Procedia Comput Sci 48:679–685

Zareapoor M, Seeja KR, Alam MA (2012) Analysis of credit card fraud detection techniques: based on certain design criteria. Int J Comput Appl 52:35–42