JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 05 Issue 01
2023

Research Article
https://doi.org/10.56979/501/2023

Detection of Credit Card Fraud Through Machine Learning In Banking Industry

Mohsin Asad Gill[1*], Muneera Quresh[2], Awais Rasool[3], and Muhammad Mubashir Hassan[4]

[1]School of Business, University of Southern Queensland, Australia.
[2]Department of Management Sciences, Qurtaba University, Peshawar, Pakistan.
[3]Department of Computer Science, University of Agriculture Faisalabad, 38000, Pakistan.
[4]Department of Computer Science, Riphah International University, Lahore, Pakistan.
[*]Corresponding Author: Mohsin Asad Gill. Email: mag_gill@hotmail.com.

Received: April 28, 2023 **Accepted:** May 19, 2023 **Published:** June 05, 2023.

Abstract: Financial fraud seems to be increasing day by day at a greater pace which impacted the economy, several collaborative institutions, and administrations. CC transactions are expanding quicker due to the progression in web innovation, which prompts high reliance on Internet banking. Through the up-degree of innovation and expansion in the utilization of CCs, misrepresentation charges result in an economic challenge. The purpose is to recognize the machine learning techniques for false CCs usage and transactions through the utilization of advanced practices based on artificial intelligence, to prevent fraudsters from the unapproved use of clients' records. Rapid growth in CC fraud is recorded worldwide, leading to the urge to act against fraudsters. Qualitative synthesis was applied to explore the techniques used in the banking industry to prevent these frauds. Putting a cutoff for those activities would undoubtedly affect the clients as their cash would be recuperated and recovered once more into their records, and they would not be charged for things or maintenance that were not bought by them, which is the principal objective of the venture. For fraudulent detection purposes, different techniques exist as machine learning, which mainly includes logistic learning, KNN, and SVM. Those machine learning models were exceedingly used for the detection of CC frauds.

Keywords: Machine Learning; Banking Industry; CC; Fraud Detection.

1. Introduction

The With the escalation of individuals utilizing credit cards (CC) in their regular routines, CC organizations ought to take exceptional consideration in the security and well-being of their clients. In 2019, almost 2.8 billion individuals were using MasterCard around the world; likewise, clients, including a ratio of 70%, own a solitary card in any event. CC misrepresentation in the US rose by 44.7% from 271,927 in 2019 to 393,207 reports in 2020. The misrepresentation regarding CC is sorted into two sets; one exists to open an account in their own name for character cheat, and reports of this deceitful behavior expanded by 48% from 2019 to 2020 (Hussein et al., 2021). The subsequent sort is by an identity cheat utilizing a current record that you made, and it's generally finished by taking the data of the card, which provides details regarding this kind of extortion expanded by 9% from 2019 to 2020 (Daly, 2021). Those insights grabbed my eye as the numbers are expanding definitely and quickly over time, which allows the consumers to identify the logic to attempt and to determine the dispute systematically by utilizing different advanced strategies to recognize the CC false exchanges inside various exchanges (Zareapoor et al., 2012).

1.1 Purpose of the Study

The article is designed to explore the techniques to detect fake or false transactions; it is significant to sort the false contacts so clients don't get indicted for the acquisition of items they are unaware of. A variety of detection models are used for securing CC; these models are machine learning techniques. These models

examine bugs and algorithms to detect, but each model has some consequences and results to find out the best-suited model for transactions through the proposed literature.

1.2 Methodology

There are various systems to detect CC frauds; for analysis, qualitative narrative synthesis was adopted to determine which applications are the most used for fraudsters and securing CC usage. This method summarizes and explains the details of famous machine-learning detection applications.

2. Related Studies

Multiple techniques were utilized by Zareapoor as well as his research fellows to decide the best working model for distinguishing deceitful money transfers, which was laid out utilizing the precision of the model, the hustle in identifying, and the expense. Several models were used, which included Bayesian network, KNN, Neural network, SVM, and much supplementary. A comparison table provided in this article depicted that the most accurate and efficient network in finding fraudulent transactions was Bayesian Network. The NN performed excellently, and the recognition was quick, with mediocre precision. KNN's haste was great, with a medium exactness. Lastly, it mentioned a lower score in SVM, speed relates to it slow than others, and medium precision existed. Concerning the expense, all models assembled were sweeping (Zareapoor et al., 2012).

It was proposed by Mailini and Pushpa that involving KNN as well as outlier detection in distinguishing card misrepresentation, the creators found in the wake of playing out their model over examined information, that the fittest technique in recognizing and deciding target instance irregularity is KNN which showed that its most fit in the detection of extortion with the memory restriction (Al-Khatib, 2012). Concerning Anomaly identification, the calculation and memory expected for the charge card extortion recognition is substantially less, notwithstanding its functioning quicker and better in enormous web-based datasets. However, KNN was more exact and effective than the results shown in the study (Malini & Pushpa, 2017).

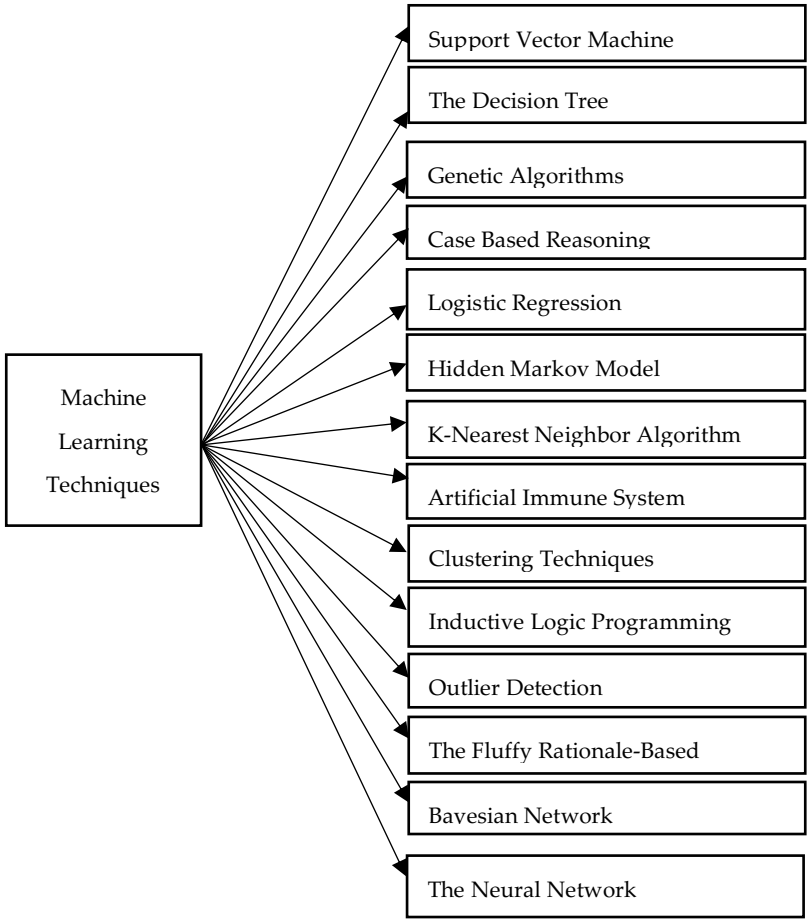

Figure 1. Analysis of literature to highlight Machine learning techniques.

3. Data Synthesis

Table 1. ML Techniques

ML Techniques	Widely used suggested applications
Support Vector Machine	Ghosh and Reilly made a model that used the SVMs and valued the brain frameworks. In this assessment, three-layer feed-forward RBF neural frameworks associated with recognizing counterfeit charge card trades, through only two passes are expected to create a distortion score predictably (Lu & Ju, 2011; Gyamfi & Abdulai, 2018; Zhang et al., 2020; Li et al., 2021).
The Decision Tree	Hub followed by additional hubs or just a single hub that is doled out by the characterization to avoid extortion (Monedero et al., 2012; Şahin & Duman, 2011; Husejinovic, 2020).
Genetic Algorithms	GA is utilized in information mining, for variable determination, the most part combined with other DM calculations (Duman & Ozcelik, 2011; Hassan et al., 2007; Benchaji et al., 2019).
Case Based Reasoning	In CBR, cases present as depictions of the involvement of the clients, besides, being set aside in a data set which utilizes for later recuperation when the client encounters one more case with tantamount boundaries (Jain et al., 2019)
Logistic Regression	Data mining tasks has a progressively more authentic model that incorporates discriminant assessment, relapse examination, and various strategic relapse (Itoo et al., 2021; Hussein et al., 2021).
Hidden Markov Model	This Markov Model is a twofold introduced stochastic interaction, which is used to display essentially more confounded stochastic cycles when diverged from an ordinary Markov model (Bhusari & Patil, 2011; Gandhi et al., 2011; Agbakwuru & Elei, 2021; Goud & Premchand, 2019).
K-Nearest Neighbor Algorithm	A champion among the best classifier calculations that have been used in the MasterCard misrepresentation discovery is the k calculation, which is a managed learning calculation (Hussein et al., 2021; Ruchitha et al ., 2022)
Artificial Immune System	AIS had various sorts of uses, including the discovery of false money-related trades. Additionally, the AIS discovery engines realize the AIS-based calculations which can bunch input data as run-of-the-mill or fake (Brabazon et al., 2010; Gadi et al., 2008; Soltani et al., 2012; Ali et al., 2020).
Clustering Techniques	The Breakpoint assessment in light of the trades of a single card, and can recognize dubious direct (Ahmed et al., 2023).
Inductive Logic Programming	Inductive Rationale Programming (ILP) and the direct put-together classifiers for social data sets (Kumar, 2021).

Outlier Detection	Anomalies are a fundamental kind of nonstandard thought that can be used for extortion recognition (Caroline Cynthia & Thomas George, 2021; Marella et al., 2019)
The Fluffy Rationale-Based Framework	It depicts the usage of a groundbreaking fluffy structure fit for organizing dubious and non-dubious CC trades. In this way, the construction includes two essential parts: a Genetic Programming (GP) look calculation and a fluffy expert system (Haratinik et al., 2012; Hussein et al., 2021).
Bayesian Network	Bayesian conviction networks are quantifiable systems in data digging and are very effective for showing conditions, where little information is presently known and it is dubious or to a limited extent unavailable to move toward data (Lee & Jo, 2010; Maes et al., 2002; Kumar et al., 2020).
The Neural Network	The proposed framework contains three coatings of programmed restricting designs. In neural network was applied to recognize the extortion in the card: spiral base capability network that is applied normally to the errands of examples (Brause et al., 1999; Chen & Lei, 2021; Esenogho et al., 2022)

3.1 Data Synthesis and Relative Discussion

The Neural Network; developing a framework for information extraction given the neurological organization to spot extortion in MasterCard (Brause et al., 1999; Ghosh & Reilly, 1994). In addition, the suggested (CARD WATCH) framework includes three levels of programmed restriction designs. Additionally, they prepared and assessed the framework using a sizable amount of organized data. As a result, the findings showed that misrepresentation was successfully detected in many cases (Bhattacharyya et al., 2011). Another model to differentiate continuous extortion is that of Krenker et al. (2009) because of the bidirectional neural organizations. In this technique, they used significant phone exchange data provided by the credit card company. It also implied that the framework would perform better than a computation based on the accepted level of false-positive rate. Using a Granular Neural Network (GNN) is suggested to speed up information finding and data mining to distinguish card extortion.

Additionally, it belongs to a class of FNNKDs, or finite neural networks reliant on information disclosure. It was separated from the SQL Server data set comprising Visa Card transactions to pre-process the core informative index for fraud detection. Therefore, they made fewer preparation mistakes than usual because more preparation data was available. Processes that are self-managed and half-breed controlled. Numerous specialists have used hybrid models in addition to the directed and autonomous learning models from neural organizations. John Chong Lait claims that the reward foundation was altered from the SICLN model to the ICLN model to update the punishment and reward loads. This advancement was also followed by an improvement in health and a reduction in preparation time.

Additionally, the quantity of essential ICLN gatherings is unrelated to the quantity of crucial neurons within the network. As a result, inoperative neurons can be removed from the blocks by employing the punishment rule. Since the SICLN performs better than the widely used unassisted conglomeration computations, the results show that both the ICLN and the SICLN are applied successfully (Stolfo et al., 1997; Stolfo et al., 2000).

The Decision Tree: The C4.5 procedure, the ID3 technique, and the decision tree (Quinlan, 1986), which could handle infinite data (Ahin & Duman, 2011), were developed after the concept of the learning framework was introduced. A decision tree is a table with nodes that may be accessed and connected by lines. Each hub is a sub-hub, followed by additional hubs or a single hub assigned by the characterization. Comparability trees produced results that could be seen when used to select trees, especially when used to organize interruption locations for a different type of extortion (Monedero et al., 2012).

Genetic Calculations: Recently, they have applied to streamline the boundaries of the backing vector machine, which was first presented by Holland (1975) for bankruptcy prediction, amalgamation with neural network for accurately identifying card extortion, and then it has been used in conjunction with the Fake Safe Framework to lessen the amount of misleading problem in MasterCard misrepresentation detection (Duman & Ozcelik, 2011). According to Hassan et al. (2007), as long as the number of alerts does not outperform a particular aspect, the current assessments of these boundaries have been resolved, the essential characteristics have been identified, the enlightening list boundaries and expansions of the number of real cautions have been made.

Case-Based Reasoning: The most fundamental component of case-based reasoning (CBR) is changing one's path of action to address one's previous problems and apply solutions to new ones. Cases in CBR can be used for request purposes, serving as representations of the client's engagement, and being kept in a data set for subsequent recovery when the client encounters a related case (Pun & Lawryshyn, 2012). When a new issue arises, a CBR system tries to determine what is happening. In this process, the model is referred to as the planning data. When a new case or model is submitted to the model during the test phase, it thoroughly analyzes all of the data to find a subset of cases that are practically equivalent to the new situation and utilizes those cases to anticipate the outcome. Although CBR is frequently associated with the closest neighbor coordinating algorithm, there are a number of other algorithms that are employed in conjunction with this process, such as Case-based reasoning, which has been extensively documented as the design for mutt misrepresentation discovery systems (Edge & Sampaio, 2009). It also linked a cross-philosophical variant of CBR and NN, which divided the task of extortion recognition into two separate pieces, and found that this diversified philosophy was more dynamically resilient than any other approach. On a case base of 1606 cases, the CBR and ANN systems claimed a plan accuracy of 89% (Ravisankar et al., 2011).

Clustering Technique: Bolton and Hand (2002) suggest two clustering methods for analyzing social misrepresentation. Companion bundle analysis is a structure that distinguishes between accounts acting unusually and accounts acting similarly at one point in time. If these records are questionable, misrepresentation inspectors are then used to find these instances. According to the principle behind buddy pack evaluation, a record must be accounted for if it is noticed that one account has performed in a way that is mostly unexpected following a period of comparable behavior. According to an alternative philosophy called Breakpoint evaluation, if a difference in card usage can be traced to a single reason, the record needs to be looked into (Prodromidis & Stolfo, 1999). Alternatively, we may state that the Breakpoint evaluation can identify dubious direct based on a single card's transactions. A sudden transaction for a significant sum and a high frequency of transactions without the cardholders' awareness are warning signs of suspect direct marketing.

Inductive Logic Programming: Inductive Logic Programming uses first solicitation predicate logic and a sizable number of positive and negative models to represent a notion. Additionally, asking for new dates is used. Complex relationships between items or qualities can be depicted using this technique. The system's capacity is improved by drawing space data more closely to an ILP structure. Muggleton and De Raedt (1994) created a model that applies the name of the data in distortion location using social learning techniques like Inductive Rational Programming (ILP) and the directly put-together classifiers for social data sets. It focuses on methods for standardizing subordinate identification about the social learning problem.

K-Nearest Neighbor Calculation: Several eccentricity location techniques have used the K-Nearest Neighbor calculation. The k-closest neighbor calculation, a controlled learning calculation in which the final result of a new case request is asked given a bigger fraction of the K-Nearest Neighbor order, is a champion among the best classifier calculations employed in the MasterCard misrepresentation discovery. It was first described in 1991 by Aha, Kibler, and Albert. Three key variables influence the division metric utilized in the KNN calculation to determine the nearest neighbors. The division rule was applied to obtain a representation from a k-nearest neighbor. The number of neighbors that the new model was defined.

Logistic regression or Calculated Relapse: Data mining tasks have a model that integrates discriminant analysis, relapse analysis, and numerous strategic relapses. This model is known as logistic regression or calculated relapse. Therefore, logistic regression (LR) is useful when we wish to have the choice to forecast the existence or absence of a brand name or outcome based on a wide range of market parameters (Raj & Portia, 2011). Although it is an immediate relapse model, it is fitted to models with dependent variables

that are dichotomous. Strategic relapse coefficients apply to a larger range of examination situations than feature examination and can be used to evaluate chance extents for all free figures in the model. Probability studies on the odds of a company failing (Ohlson, 1980; Martin, 1997).

Outlier Detection: An important category of unconventional thinking that can be used to identify extortion is anomalies. The Exception used in this model is a review that dramatically deviates from other discernments and raises the question of whether a discretionary instrument carried it out. Unassisted learning typically produces an additional explanation or representation of the observed data, improving future decisions (RamaKalyani & UmaDevi, 2012). The approaches used are easily able to discriminate between legal transactions and extortion that have lately come to light. Using social anomaly recognition tools, Bolton and Hand have suggested several unassisted strategies for locating Visa extortion. Cases of probable misrepresentation will be recognized as spending patterns that depart from the norm and repeat in transactions (Stolfo et al., 1997; Stolfo et al., 2000).

Support Vector Machine: The Support Vector Machine (SVM) is a matched classifier and supervised learning model that can distinguish between and view plans for gathering and backsliding tasks. In their match of the assistance vector system (BSVS) proposal, Tung-Shou Chen et al. used Genetic Algorithms (GA) techniques to select the assistance vectors. According to the proposed approach (thin & Duman, 2011; Delamaire et al., 2009), a self-determining map (SOM) was first linked to securing a high regrettable rate, and the BSVS was then utilized to prepare the data consistent with their conveyance. A decision tree and support vector machine (SVM) based model for identifying Visa fraud was also developed. This study compared SVM and decision tree methods for control card extortion, and the results are unquestionably instructive. Despite this, the outcomes showed that Truck and other decision tree classifiers performed better than SVM when the issue was closely scrutinized. To replace the (QRT) technique with the SVM for credit card distortion identifiable proof, Tiwari et al. (2021) advised an original review respondent (Lu & Ju, 2011). This study aimed to evaluate the SVM's accuracy in calculating figures in the coercion area compared to other systems, such as over-analyzing and a higher percentage of votes cast. The results of the trial showed that the QRT technique is quite efficient in terms of assumption accuracy. Due to the enormous dimensionality of the data, Principal Component Analysis (PCA) was initially used by Qibei Lu et al. to condense data estimation to a smaller set of composite features. An improved Trim sidedness Class Weighted SVM (ICW-SVM) was proposed in light of the intricacy of the data. The quantitative learning technique known as Help Vector Machines (SVM) has several useful applications for a variety of issues. It was also first introduced by Cortes and Vapnik (1995), and Panigrahi et al. (2009) underlined its applicability in several collection-related activities.

Bayesian Network: Cooper and Herskovits (1992) first described the Bayesian conviction network. The effectiveness of Bayesian conviction networks for illustrating circumstances where little information is currently known, and it is unknown or largely unavailable to advance toward data can be quantified. Despite this, the goal of applying Bayesian standards is to foresee a precise assessment of a discrete class variable that has been delegated given a vector of signs or features. Sam Maes and three individuals were recommended for BN recognition in 1993 for credit card extortion. To spot misrepresentation, Chaudhary et al. (2012) and Maes et al. (2002) created two Bayesian organizations for expressing the direction of clients. The Bayesian Organization requires intensive data maintenance and planning. The neural network is slower when connected to novel events than the BN, which is more accurate and much faster. The fake customer leads, and the real (typical) client lead are two credit card fraud tactics highlighted in other studies using Bayesian organization (Lee & Jo, 2010). The dishonest lead net is created using master learning, and the authenticate is set up to allow access to client data even when they are not trying to conduct fraud. A particular client's needs and expanding data change the actual lead net. By placing it in the space between the two organizations and then examining the probability, Lei and Ghorbani (2012) determined the depiction of new transactions. When put into practice, Bayes's standard gives the likelihood of distortion for novel transactions. Ezawa and Norton developed a four-organize Bayesian organization again because they felt that several popular techniques, such as backslide, K-nearest neighbor, and neural organizations, took too long to absorb their data (Li et al., 2021).

Hidden Markov Model: In comparison to a traditional Markov model, this Markov model uses a double-introduced stochastic interaction to depict substantially more intricate stochastic cycles. An impending

credit card transaction is deemed fraudulent if a preset Hidden Markov Model cannot identify it with a high enough probability (Bhusari & Patil, 2011).

The Fluffy Rationale-Based Framework: Due to its hazy rules, FLBS is the organization. By displaying hazy sets and numbers and communicating values as etymological variables, such as almost nothing, medium, and huge, it tends to increase the vulnerability of the data and yield factors (Haratinik et al., 2012). The Fluffy Brain Organization (FNN) and the Fluffy Darwinian Framework (FDS) are two important subtypes of these Organizations. Fluffy Neural Structure (FNN): FNNs process enormous amounts of confusing data in every part of our lives. Syeda et al. (2002) claim that "fluffy neural networks on identical machines" can hasten creating rules for detecting client express credit card fraud.

Additionally, his work relates to Data mining and Information Disclosure in database systems." In this method, Syeda et al. used a GNN (Granular Neural Network) procedure that uses a fuzzy brain network based on information disclosure (FNNKD) to determine how quickly the organization can be established and how quickly distinct clients can be handled for identification. Various fields in the trade table consolidate trade aggregates, time between trades, decree date, trade code, posting date, and trade depiction (Haratinik et al., 2012; Hussein et al., 2021). As is customary for the execution of this card misrepresentation detection strategy, the material fields from the data set were eradicated using a valid SQL examination, resulting in a successful encounter. Fluffy Darwinian Framework (FDS), this method employs Hereditary programming to develop fluffy rationale rules and to be suitable for classifying MasterCard transactions into "dubious" and "not-dubious" categories (Hussein et al., 2021).

The artificial Immune system addresses Neal et al.'s (1998) massive strategy fueled by natural frameworks. Nonetheless, one of the most important tendencies of the AIS model is that model requires only a few advisers to be prepared, thereby producing locators (ALCs) with a negative determination technique (Brabazon et al., 2010). These systems are a category of bio-motivated adaptable or learning calculations that incorporate the fake resistant confirmation framework, a directed finding that has demonstrated tremendous success on the representation issue in the MasterCard misrepresentation discovery, and this strategy can address the collection issue in brain organization (Gadi et al., 2008). The framework produces an ALC at its discretion, tests it against the strategy of self-examples, and if it does not organize any of its models, it is incorporated into the strategy of fostering ALCs (Soltani et al., 2012; Wong et al., 2012). The Artificial Immune System (AIS) contains artificial lymphocytes (ALCs) that are able to portray any model as self or non-self by recognizing only non-self-models. The AIS has also been utilized in PC security to differentiate network interference, group data for data mining, identify PC contaminations, and recognize thought learning. Then, the uncommon state model of AIS was linked to recognizing credit card extortion, which was primarily influenced by Hofmeyr and Forrest (1999) and Wightman (2003). The most significant advances in AIS have centered on the following five immunological hypotheses: clonal selection, resistant organizations, risk hypothesis, hybrid AIS, and negative determination.

4. Conclusions

There are so many techniques also which might use in the detection of CC frauds dataset for charge card misrepresentation recognition (CCFD). The techniques could be improved to obtain improved results. Additionally, utilizing our measurements might measure up to different procedures like Arbitrary Backwoods, SVC, Choice Braid, neural Organization, and Genetic Calculation. The primary restriction of Arbitrary Under-testing accomplishing ideal outcomes which can demonstrate support in CC misrepresentation identification in the future. Similarly, our outcomes may be valuable and can offer further assistance to the relationship to gather an immeasurably superior charge card misrepresentation discovery framework (CCFDS) which can better manage the slanted data and use better estimations to survey the results.

References

1. Agbakwuru, A. O., & Elei, F. O. (2021). Hidden Markov model application for CC fraud detection systems. International Journal of Innovative Science and Research, 5(1), 2020.
2. Ahmad, H., Kasasbeh, B., Aldabaybah, B., & Rawashdeh, E. (2023). Class balancing framework for CC fraud detection based on clustering and similarity-based selection (SBS). International Journal of Information Technology, 15(1), 325-333.
3. Ali, I., Aurangzeb, K., Awais, M., & Aslam, S. (2020, November). An efficient CC fraud detection system using deep-learning based approaches. In 2020 IEEE 23rd International Multitopic Conference (INMIC) (pp. 1-6). IEEE.
4. Al-Khatib, A. M. (2012). Electronic payment fraud detection techniques. World of Computer Science and Information Technology Journal, 2(4), 137-141.
5. Benchaji, I., Douzi, S., & El Ouahidi, B. (2019). Using genetic algorithm to improve classification of imbalanced datasets for CC fraud detection. In Smart Data and Computational Intelligence: Proceedings of the International Conference on Advanced Information Technology, Services and Systems (AIT2S-18) Held on October 17–18, 2018 in Mohammedia 3 (pp. 220-229). Springer International Publishing.
6. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for CC fraud: A comparative study. Decision support systems, 50(3), 602-613.
7. Bhusari, V., & Patil, S. (2011). Application of hidden markov model in CC fraud detection. International journal of distributed and parallel systems, 2(6), 203.
8. Brabazon, A., Cahill, J., Keenan, P., & Walsh, D. (2010, July). Identifying online CC fraud using artificial immune systems. In IEEE Congress on Evolutionary Computation (pp. 1-7). IEEE.
9. Brause, R., Langsdorf, T., & Hepp, M. (1999, November). Neural data mining for CC fraud detection. In Proceedings 11th International Conference on Tools with Artificial Intelligence (pp. 103-106). IEEE.
10. Caroline Cynthia, P., & Thomas George, S. (2021). An outlier detection approach on CC fraud detection using machine learning: a comparative analysis on supervised and unsupervised learning. In Intelligence in Big Data Technologies—Beyond the Hype: Proceedings of ICBDCC 2019 (pp. 125-135). Springer Singapore.
11. Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of fraud detection techniques: CC. International Journal of Computer Applications, 45(1), 39-44.
12. Chen, J. I. Z., & Lai, K. L. (2021). Deep convolution neural network model for credit-card fraud detection and alert. Journal of Artificial Intelligence and Capsule Networks, 3(2), 101-112.
13. Daly, L. (2021). Identity theft and CC fraud statistics for 2021: the ascent. The Motley Fool.
14. Delamaire, L., Abdou, H., & Pointon, J. (2009). CC fraud and detection techniques: a review. Banks and Bank systems, 4(2), 57-68.
15. Duman, E., & Ozcelik, M. H. (2011). Detecting CC fraud by genetic algorithm and scatter search. Expert Systems with Applications, 38(10), 13057-13063.
16. Edge, M. E., & Sampaio, P. R. F. (2009). A survey of signature based methods for financial fraud detection. computers & security, 28(6), 381-394.
17. Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A neural network ensemble with feature engineering for improved CC fraud detection. IEEE Access, 10, 16400-16407.
18. Gadi, M. F. A., Wang, X., & do Lago, A. P. (2008, August). CC fraud detection with artificial immune system. In International conference on artificial immune systems (pp. 119-131). Berlin, Heidelberg: Springer Berlin Heidelberg.
19. Gandhi, B. S., Naik, R. L., Krishna, S. G., & Lakshminadh, K. (2011). Markova Scheme for CC Fraud Detection. In International Conference on Advanced Computing, Communication and Networks (pp. 144-147).
20. Ghosh, S., & Reilly, D. L. (1994, January). CC fraud detection with a neural-network. In System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on (Vol. 3, pp. 621-630). IEEE.
21. Goud, V. S., & Premchand, P. (2019). ENHANCED HIDDEN MARKOV MODEL FOR CC FRAUD DETECTION. Complexity International, 23(2).
22. Gyamfi, N. K., & Abdulai, J. D. (2018, November). Bank fraud detection using support vector machine. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 37-41). IEEE.
23. Hansen, J. V., Lowry, P. B., Meservy, R. D., & McDonald, D. M. (2007). Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. Decision Support Systems, 43(4), 1362-1374.
24. Haratinik, M. R., Akrami, M., Khadivi, S., & Shajari, M. (2012, November). FUZZGY: A hybrid model for CC fraud detection. In 6th international symposium on telecommunications (IST) (pp. 1088-1093). IEEE.
25. Hofmeyr, S. A. (1999). An immunological model of distributed detection and its application to computer security (Doctoral dissertation, The University of New Mexico).
26. Husejinovic, A. (2020). CC fraud detection using naive Bayesian and c4. 5 decision tree classifiers. Husejinovic, A.(2020). CC fraud detection using naive Bayesian and C, 4, 1-5.
27. Hussein, A. S., Khairy, R. S., Najeeb, S. M. M., & Alrikabi, H. T. S. (2021). CC Fraud Detection Using Fuzzy Rough Nearest Neighbor and Sequential Minimal Optimization with Logistic Regression. International Journal of Interactive Mobile Technologies, 15(5).

28. Itoo, F., Meenakshi, & Singh, S. (2021). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for CC fraud detection. International Journal of Information Technology, 13, 1503-1511.
29. Jain, Y., Tiwari, N., Dubey, S., & Jain, S. (2019). A comparative analysis of various CC fraud detection techniques. International Journal of Recent Technology and Engineering, 7(5), 402-407.
30. Krenker, A., Volk, M., Sedlar, U., Bešter, J., & Kos, A. (2009). Bidirectional Artificial Neural Networks for Mobile-Phone Fraud Detection. Etri Journal, 31(1), 92-94.
31. Kumar, C. V. (2021). CC FRAUD DETECTION USING AUTOENCODERS.
32. Lee, K. C., & Jo, N. Y. (2010). Bayesian network approach to predict mobile churn motivations: emphasis on general Bayesian network, Markov blanket, and what-if simulation. In Future Generation Information Technology: Second International Conference, FGIT 2010, Jeju Island, Korea, December 13-15, 2010. Proceedings 2 (pp. 304-313). Springer Berlin Heidelberg.
33. Lei, J. Z., & Ghorbani, A. A. (2012). Improved competitive learning neural networks for network intrusion and fraud detection. Neurocomputing, 75(1), 135-145.
34. Li, C., Ding, N., Zhai, Y., & Dong, H. (2021). Comparative study on CC fraud detection based on different support vector machines. Intelligent Data Analysis, 25(1), 105-119.
35. Lu, Q., & Ju, C. (2011). Research on CC fraud detection model based on class weighted support vector machine. Journal of Convergence Information Technology, 6(1).
36. Maes, S., Tuyls, K., Vanschoenwinkel, B., & Manderick, B. (2002, January). CC fraud detection using Bayesian and neural networks. In Proceedings of the 1st international naiso congress on neuro fuzzy technologies (Vol. 261, p. 270).
37. Malini, N., & Pushpa, M. (2017, February). Analysis on CC fraud identification techniques based on KNN and outlier detection. In 2017 third international conference on advances in electrical, electronics, information, communication and bio-informatics (AEEICB) (pp. 255-258). IEEE.
38. Marella, S. T., Karthikeya, K., Myla, S., Sai, M., & Allam, V. (2019). Detecting fraudulent CC transactions using outlier detection. International Journal of Scientific and Technology Research, 8(10), 630-637.
39. Monedero, I., Biscarri, F., León, C., Guerrero, J. I., Biscarri, J., & Millán, R. (2012). Detection of frauds and other non-technical losses in a power utility using Pearson coefficient, Bayesian networks and decision trees. International Journal of Electrical Power & Energy Systems, 34(1), 90-98.
40. Muggleton, S., & De Raedt, L. (1994). Inductive logic programming: Theory and methods. The Journal of Logic Programming, 19, 629-679.
41. Panigrahi, S., Kundu, A., Sural, S., & Majumdar, A. K. (2009). CC fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning. Information Fusion, 10(4), 354-363.
42. Prodromidis, A. L., & Stolfo, S. (1999). Agent-based distributed learning applied to fraud detection.
43. Pun, J., & Lawryshyn, Y. (2012). Improving CC fraud detection using a meta-classification strategy. International Journal of Computer Applications, 56(10).
44. Quinlan, J. R. (1986). Induction of decision trees. Machine learning, 1, 81-106.
45. Raj, S. B. E., & Portia, A. A. (2011, March). Analysis on CC fraud detection methods. In 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET) (pp. 152-156). IEEE.
46. RamaKalyani, K., & UmaDevi, D. (2012). Fraud detection of CC payment system by genetic algorithm. International Journal of Scientific & Engineering Research, 3(7), 1-6.
47. Ravisankar, P., Ravi, V., Rao, G. R., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. Decision support systems, 50(2), 491-500.
48. Ruchitha, G. S., Karthick, V., & Nasim, I. (2022, November). A Novel Approach to Find Accuracy in CC Fraud Detection Using Improved K-Nearest Neighbor Classifier Method Comparing with Logistic Regression Algorithm. In 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS) (pp. 1-8). IEEE.
49. Şahin, Y. G., & Duman, E. (2011). Detecting CC fraud by decision trees and support vector machines.
50. Soltani, N., Akbari, M. K., & Javan, M. S. (2012, May). A new user-based model for CC fraud detection based on artificial immune system. In The 16th CSI International Symposium on Artificial Intelligence and Signal Processing (AISP 2012) (pp. 029-033). IEEE.
51. Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. (2008). CC fraud detection using hidden Markov model. IEEE Transactions on dependable and secure computing, 5(1), 37-48.
52. Stolfo, S. J., Fan, W., Lee, W., Prodromidis, A., & Chan, P. K. (2000, January). Cost-based modeling for fraud and intrusion detection: Results from the JAM project. In Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00 (Vol. 2, pp. 130-144). IEEE.
53. Stolfo, S., Fan, D. W., Lee, W., Prodromidis, A., & Chan, P. (1997, July). CC fraud detection using meta-learning: Issues and initial results. In AAAI-97 Workshop on Fraud Detection and Risk Management (pp. 83-90).
54. Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., & Singh, A. K. (2021). CC fraud detection using machine learning: a study. arXiv preprint arXiv:2108.10005.
55. Tuo, J., Ren, S., Liu, W., Li, X., Li, B., & Lei, L. (2004, October). Artificial immune system for fraud detection. In 2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No. 04CH37583) (Vol. 2, pp. 1407-1411). IEEE.

56. Wong, N., Ray, P., Stephens, G., & Lewis, L. (2012). Artificial immune systems for the detection of CC fraud: an architecture, prototype and preliminary results. Information Systems Journal, 22(1), 53-76.
57. Zareapoor, M., Seeja, K. R., & Alam, M. A. (2012). Analysis on CC fraud detection techniques: based on certain design criteria. International journal of computer applications, 52(3).
58. Zhang, D., Bhandari, B., & Black, D. (2020). CC fraud detection using weighted support vector machine. Applied Mathematics, 11(12), 1275.