A Survey and a Credit Card Fraud Detection and Prevention Model using the Decision Tree Algorithm

Abdulaziz Saleh Alraddadi
College of Computer Science and Engineering at Yanbu, Taibah University, Saudi Arabia
alraddadi1@yahoo.com (corresponding author)

Received: 17 June 2023 | Revised: 27 June 2023 | Accepted: 1 July 2023

 DOI: https://doi.org/10.48084/etasr.6128

ABSTRACT

Today, many people prefer online payment methods due to the rapid growth in cashless electronic transactions. Credit and debit cards are the most popular electronic payment methods but are prone to fraud due to the nature of their use and the tendency of fraudsters to access their details. This study proposes a theoretical credit fraud detection and prevention model using a Decision Tree Algorithm (DCA). Moreover, a survey questionnaire was used to investigate students' perceptions of credit card fraud incidents. Data were collected from 102 students from different universities and countries around the world. The results showed that 95.9% of the respondents knew how credit/debit card fraud occurs, while 4.1% of them did not. Finally, 81.6% expressed their willingness to use a tool based on the proposed model to prevent or detect credit/debit card fraud incidents.

Keywords-online payment; credit card fraud; Decision Tree Algorithm (DCA); survey

I. INTRODUCTION

Cybercrime is one of the most serious threats cyberspace users and the global economy face. According to European and international organizations, it is considered one of the most significant security challenges of the 21st century [1]. Numerous studies have attempted to investigate or prevent cybercrime methods. Such studies contain database schemes [2], automation [3], avoiding cyberbullying [4], wireless networks [5-6], cloud safety [7-8], smart IoT [9-10], drone domain and mobile areas [11], and the health field [12-20]. Companies and organizations monitor consumers' or users' spending patterns to identify and prevent fraudulent activities. Credit cards are becoming increasingly popular as a payment method in both online and conventional transactions. Fraud detection involves the identification and capture of fraudulent activities and events. In recent decades, many modern methods have been developed to prevent frauds related to credit card transactions. Several approaches can be used to detect and prevent fraudulent transactions, including machine learning, data mining, sequence alignment, fuzzy reasoning, genetic programming, and fuzzy reasoning [21-22]. Fraud occurs when goods, services, or money are acquired illegally. There are many situations in which frauds occur when there is criminal intent present, but it is often obscure. In addition to credit cards, there are many other fraud targets. Credit card fraud is a general term for theft, fraud, and other similar payment methods used fraudulently to fund a transaction. Credit card fraud is becoming a growing problem. As it can be challenging to identify credit card fraud using standard procedures, the development of prevention models is now crucial for academic and commercial institutions. Furthermore, with the development of technology over the past few decades, fraud methods have changed dramatically. Credit card fraud is one of the greatest obstacles for business and commercial enterprises. Credit card fraud is the use of another person's credit card for private reasons without the person who owns the card or the card issuer being aware of it [23-24].

Credit card fraud can be eliminated, and financial risks can be reduced using many systems, models, procedures, and preventive measures. Although the number of people using credit cards is quickly increasing, very few feel secure and confident in using them for regular purchases [23, 25]. Credit card fraud is expanding around the world along with advancements in communication channels and information technology, leading to significant losses. This study investigated the extent to which students have been victims of credit card fraud and focused on a model to detect and prevent credit card fraud on campuses. To address this objective, four research questions (RQ) were formulated as follows:

- RQ1: Have you ever heard of or been involved in credit card fraud before?
- RQ2: How do you think it does happen?
- RQ3: How do you think it can be mitigated?
- RQ4: Would you use a solution based on the proposed model that prevents credit card fraud?

The main contribution of this study is the proposal of a theoretical framework for a model to prevent credit card fraud.

Moreover, this study investigated students' perceptions of how credit card fraud occurs and can be prevented or detected using a survey questionnaire. Finally, it was determined that the students would be willing to use such a system.

II. RELATED WORKS

In [26], an algorithmic framework was developed using a decision tree and a combination of Luhn's and Hunt's algorithms to prevent credit card fraud. Frauds were detected using Luhn's algorithms in incoming transactions, which were assessed based on address mismatches and degrees of outliers to determine how far they deviate from the typical customer profile. Bayes' theorem was applied to strengthen or weaken the general belief, and a more sophisticated combinatorial heuristic was applied to combine the probable fraud with the original belief. In [27], three methods were proposed, using machine learning algorithms to identify fraudulent transactions. Many metrics can be used to assess how well a classifier or predictor performs, such as the vector machine, the random forest, and decision trees. It is important to note that these measures depended on prevalence [28]. In [29], a comparative study was conducted among the different methods of detecting credit card fraud. In [30], three security levels were introduced in the concept of credit card fraud detection based on a Hidden Markov Model (HMM). In [31], HMMs were used to detect fraudulent card payments in two stages using dynamic random forest and k-Nearest-Neighbor algorithms. In [32], advanced data mining techniques were investigated to combine with a neural network based on real-time credit card data to offer even stronger predictive capabilities. In [33], two kinds of random forest methods were used to train features that represent normal or abnormal transactional behavior. In [34], supervised algorithms were used for the same purpose, including Deep Learning, Logistic Regression, Nave Bayesian, Support Vector Machines (SVM), Neural Networks, Artificial Immune Systems, K-Nearest Neighbor, Decision Trees, Data Mining, and Fuzzy logic-based systems. In [27, 35] prediction, clustering, and outlier identification were compared in machine learning techniques. Random forests were used to train a classifier to recognize the behavioral characteristics of credit card transactions. The following methods were used to train the genuine and fraudulent "behavior feature": CART-based random forest and random forest based on random trees. Transactions were grouped into relevant sliding window groups, and various window features were retrieved to discover consumer behavioral patterns. There are features such as the maximum or minimum amount of a transaction, average amounts in the windows, and even the time elapsed [36].

Systems generate fraud scores for specific transactions using a variety of instructions and algorithms. In [37], deep neural network techniques were proposed for fraud detection. The preparation approach is a significant setback in addressing data skew issues in a dataset. There are numerous methods to assess whether a transaction is legitimate or fraudulent [24]. The drawback of supervised learning is that it depends on people to optimize its settings. On the contrary, decision trees can be built more quickly than other techniques and do not require the user to set any parameters [26]. Although internet payments are more convenient, adequate, and easy to use, losses related to electronic commerce should not be ignored. There are many security frameworks for businesses and banks, but fraudsters change their subtle strategies over time to bypass them. Therefore, it is essential to improve methods for detection and prevention [28]. Understanding the way a fraud is carried out is essential for effective fraud prevention. A credit card fraud detection tool should depend on the fraud technique itself [38-39]. In [40-42], machine learning-based methods were used to detect fraud in financial transactions and analyze research gaps to uncover research trends in the area. In [46], some unsupervised credit card fraud detection methods were proposed with the aid of behavioral outlier identification methods. Most likely, fraud incidents will be discovered as anomalous spending patterns and transaction frequency.

TABLE I. SUMMARY OF EXISTING WORKS.

Ref	Focus
[26]	Credit cards were validated using the credit card number (input). Incoming transactions were assessed based on address mismatches and degrees of outliers to determine how far they deviate from the typical customer profile.
[27]	Many metrics were used to evaluate the performance of a classifier or predictor.
[30]	Three levels of security were introduced using a HMM
[31]	Dynamic random forest algorithms and k-nearest neighbor algorithms were used to detect credit card fraud in two stages
[32]	The possibility of improving prediction by combining advanced data mining techniques with a neural network based on real-time credit card data was investigated.
[33]	Two types of random forest methods were used. Trainning features represent normal and abnormal transaction behavior

III. THE PROPOSED MODEL

This study used design science research [43] to propose a credit fraud detection and prevention model, using a Decision Tree Algorithm (DCA). The development process consisted of three main stages, as shown in Figure 1.

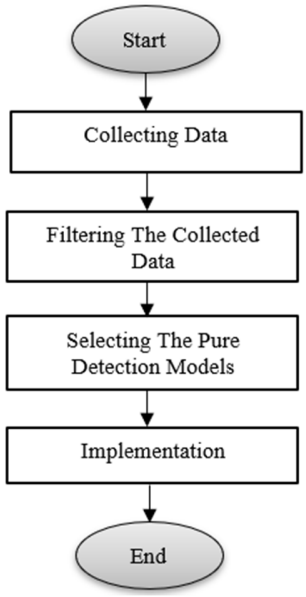

Fig. 1. Research methodology.

These stages were: collecting data, filtering the collected data, and selecting detection models for implementation. In the first stage, common search engines were used to retrieve relevant articles using the keywords "Fraud Prevention" and "Fraud Detection" for the period 2014-2023, and Kaggle was used to retrieve several credit card transaction datasets with labels for fraudulent credit card transactions. Only journal and conference papers written in English were collected. The datasets had several credit card transactions, with an additional binary field called that indicated whether a transaction was fraudulent (1) or not. The datasets also included transaction features, such as amount, time, frequency, geographic location, merchant information, cardholder information, transaction type, and device type and information. In the second stage, the collected data were filtered. A DCA was used in the design of the credit fraud detection and prevention model based on common features, as shown in Figure 2.

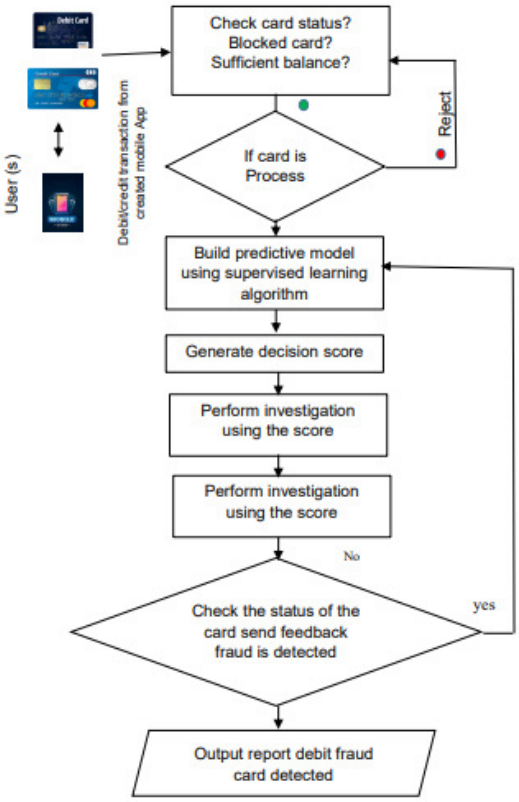

Fig. 2. The proposed credit card fraud detection and prevention model.

The model used supervised learning, specifically DCA. DCA tree-structured classification starts with a root node and divides the dataset's features into internal nodes that represent dataset features, decision instructions, and results [44]. A decision tree simply poses a query and divides it into subtrees depending on the response. Although DCA can resolve classification and regression problems, it is mostly applied to the former. The method starts its search at the top of the tree to locate the dataset classes. To reach the next node, it calculates the branch based on the relations and matches the base trait with the record attribute [45]. As shown in Figure 2, the proposed model was designed to work on the user's device as a client-side implementation to forecast the possibility of fraud. Based on the forecast made by the model, the user gets real-time feedback regarding the transaction risk level. If the model detects a high likelihood of fraud, the user may receive a warning. The model should be compatible with Android, iOS, and PC operating systems. Credit or debit card transactions were assumed to take place over the Internet, at a sales point, or in a mobile application. At the initiation of the transaction, the card status is checked, and the transaction proceeds if the card is valid. The model uses DCA, the expected score is generated, the investigation is carried out, and the appropriate decision is taken. If the score is appropriate, the card status is further checked. If a fraudulent trace is noticed, it automatically rejects the transaction, otherwise it is executed and outputs successfully.

The second phase used a questionnaire that was distributed through the WhatsApp platform, targeting a population of 450 students. The adopted questionnaire design was vetted by an expert and 102 responses were recovered within 48 hours. The purpose of the survey was to obtain responses that will provide answers to research questions. The proposed model was discussed with the respondents before sending the questionnaires.

IV. SURVEY

The survey was carried out among computer science students. Figure 3 shows the ages of the respondents, where 79.6% were 21-30 years old, and 20.4% were 11-20 years old, and Figure 4 shows the degree levels of the participant students.

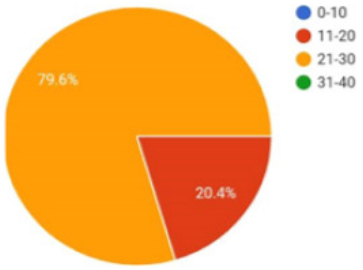

Fig. 3. Ages of respondents.

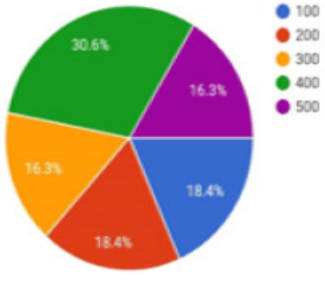

Fig. 4. Respondents' degree levels.

Figure 5 shows that 95.9% of the respondents had knowledge of how frauds occur through credit or debit cards, while 4.1% of them did not. On the other hand, as shown in Figure 6, 67.3% answered "others" for the sources of fraud incidents. However, 20.4% responded that it occurs online and 12.3% agreed that it often happens through POS, ATM, and mobile applications.

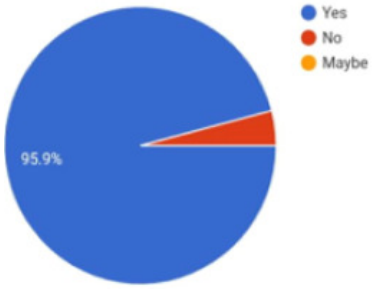

Fig. 5. Knowledge about credit card fraud.

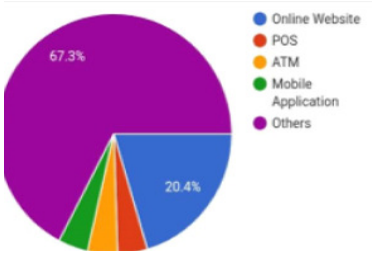

Fig. 6. Medium for credit card fraud.

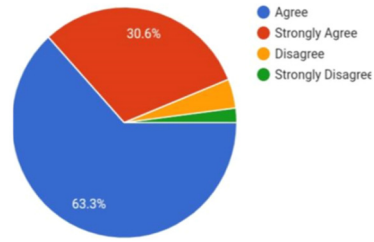

Fig. 7. Students that believe in the use of a solution that prevents credit card fraud.

Figure 5 answers RQ1, while Figure 6 answers RQ2. As shown in Figure 7, the vast majority of respondents agreed that a method that can prevent or detect debit/credit card fraud is needed. Developing a solution is one thing, but using it is another. Figure 7 shows that 63.3% of the respondents expressed their willingness to use such a method based on the proposed model to prevent or detect credit/debit card fraud, while 30.6% of the respondents strongly welcome such a solution. Meanwhile, 7.1% did not believe that such a solution could minimize the risk of credit card fraud. These results answer RQ4. Below are the solutions suggested by the students that can help in resolving the issue of credit card fraud in addition to the proposed model, providing further answers to RQ3:

- Developing a system that uses fingerprint before card details are requested to identify the user of the mobile application or on-site.
- Other personal details of the user should be required in online transactions rather than the serial number of the card and CVV.
- Cyber-security awareness should be consolidated for everyone, including students and business owners.
- Individuals should be careful when using credit cards online, especially when certain malware can be easily installed unknowingly, such as keyloggers or spyware.
- The ability of access to customers' details after a withdrawal at POS centers should be disabled.
- Educating people about not disclosing their details and avoiding visiting sites that are not secure.

V. CONCLUSION

Credit card fraud is an issue that has received a lot of attention during the recent years. This study presented a theoretical model to minimize the challenges associated with credit card fraud and surveyed the perspectives of university students. This study also provides insight into the willingness of the respondents to use a method that will provide such prevention measures. As a result of the study, information was obtained from selected university groups of students and the results indicate that students are very positive about using a method based on the proposed model. Furthermore, the study offers suggestions that could help prevent users from being scammed by debit/credit card fraud. In the future, the proposed model could be developed and tested in a real-world scenario.

REFERENCES

[1] G. Meško, "On Some Aspects of Cybercrime and Cybervictimization," *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 26, no. 3, pp. 189–199, Aug. 2018, https://doi.org/10.1163/15718174-02603006.

[2] A. Al-Dhaqm, W. M. S. Yafooz, S. H. Othman, and A. Ali, "Database Forensics Field and Children Crimes," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. Cham, Switzerland: Springer International Publishing, 2023, pp. 81–92.

[3] M. Q. Mohammed *et al.*, "Deep Reinforcement Learning-Based Robotic Grasping in Clutter and Occlusion," *Sustainability*, vol. 13, no. 24, Jan. 2021, Art. no. 13686, https://doi.org/10.3390/su132413686.

[4] W. M. S. Yafooz, A. Al-Dhaqm, and A. Alsaeedi, "Detecting Kids Cyberbullying Using Transfer Learning Approach: Transformer Fine-Tuning Models," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. Cham, Switzerland: Springer International Publishing, 2023, pp. 255–267.

[5] I. U. Onwuegbuzie, S. A. Razak, I. F. Isnin, A. Al-dhaqm, and N. B. Anuar, "Prioritized Shortest Path Computation Mechanism (PSPCM) for wireless sensor networks," *PLOS ONE*, vol. 17, no. 3, 2022, Art. no. e0264683, https://doi.org/10.1371/journal.pone.0264683.

[6] A. Al-dhaqm, M. Bakhtiari, E. Alobaidi, and A. Saleh, "Studding and Analyzing Wireless Networks Access points," *International Journal of Scientific & Engineering Research*, vol. 4, no. 1, Jan. 2013.

[7] R. Al-Mugerrn, A. Al-Dhaqm, and S. H. Othman, "A Metamodeling Approach for Structuring and Organizing Cloud Forensics Domain," in *2023 International Conference on Smart Computing and Application*

(ICSCA), Hail, Saudi Arabia, Oct. 2023, pp. 1–5, https://doi.org/10.1109/ICSCA57840.2023.10087425.

[8] A. A. Zubair *et al.*, "A Cloud Computing-Based Modified Symbiotic Organisms Search Algorithm (AI) for Optimal Task Scheduling," *Sensors*, vol. 22, no. 4, Jan. 2022, Art. no. 1674, https://doi.org/10.3390/s22041674.

[9] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology," *Engineering, Technology & Applied Science Research*, vol. 10, no. 2, pp. 5441–5447, Apr. 2020, https://doi.org/10.48084/etasr.3394.

[10] M. Saleh *et al.*, "A Metamodeling Approach for IoT Forensic Investigation," *Electronics*, vol. 12, no. 3, Jan. 2023, Art. no. 524, https://doi.org/10.3390/electronics12030524.

[11] A. E. Yahya, A. Gharbi, W. M. S. Yafooz, and A. Al-Dhaqm, "A Novel Hybrid Deep Learning Model for Detecting and Classifying Non-Functional Requirements of Mobile Apps Issues," *Electronics*, vol. 12, no. 5, Jan. 2023, Art. no. 1258, https://doi.org/10.3390/electronics12051258.

[12] K. N. Qureshi *et al.*, "A Blockchain-Based Efficient, Secure and Anonymous Conditional Privacy-Preserving and Authentication Scheme for the Internet of Vehicles," *Applied Sciences*, vol. 12, no. 1, Jan. 2022, Art. no. 476, https://doi.org/10.3390/app12010476.

[13] A. Al-dhaqm, "Detection and prevention of malicious activities on RDBMS relational database management systems," *International Journal of Scientific & Engineering Research*, vol. 3, no. 9, Sep. 2012.

[14] I. U. Onwuegbuzie, S. A. Razak, I. F. Isnin, T. S. J. Darwish, and A. Al-dhaqm, "Optimized backoff scheme for prioritized data in wireless sensor networks: A class of service approach," *PLOS ONE*, vol. 15, no. 8, 2020, Art. no. e0237154, https://doi.org/10.1371/journal.pone.0237154.

[15] S. Abd Razak, N. H. Mohd Nazari, and A. Al-Dhaqm, "Data Anonymization Using Pseudonym System to Preserve Data Privacy," *IEEE Access*, vol. 8, pp. 43256–43264, 2020, https://doi.org/10.1109/ACCESS.2020.2977117.

[16] W. A. H. Altowayti *et al.*, "The Role of Conventional Methods and Artificial Intelligence in the Wastewater Treatment: A Comprehensive Review," *Processes*, vol. 10, no. 9, Sep. 2022, Art. no. 1832, https://doi.org/10.3390/pr10091832.

[17] M. Rasool, N. A. Ismail, A. Al-Dhaqm, W. M. S. Yafooz, and A. Alsaeedi, "A Novel Approach for Classifying Brain Tumours Combining a SqueezeNet Model with SVM and Fine-Tuning," *Electronics*, vol. 12, no. 1, Jan. 2023, Art. no. 149, https://doi.org/10.3390/electronics12010149.

[18] M. Q. Mohammed *et al.*, "Review of Learning-Based Robotic Manipulation in Cluttered Environments," *Sensors*, vol. 22, no. 20, Jan. 2022, Art. no. 7938, https://doi.org/10.3390/s22207938.

[19] I. U. Onwuegbuzie, S. A. Razak, and A. Al-Dhaqm, "Multi-Sink Load-Balancing Mechanism for Wireless Sensor Networks," in *2021 IEEE International Conference on Computing (ICOCO)*, Kuala Lumpur, Malaysia, Aug. 2021, pp. 140–145, https://doi.org/10.1109/ICOCO53166.2021.9673578.

[20] D. M. Bakhtiari and A. M. R. Al-dhaqm, "Mechanisms to Prevent lose Data," *International Journal of Scientific & Engineering Research*, vol. 3, no. 12, Dec. 2012.

[21] K. Chaudhary, J. Yadav, and B. Mallick, "A review of Fraud Detection Techniques: Credit Card," *International Journal of Computer Applications*, vol. 45, no. 1, pp. 39–44, May 2012.

[22] A. A. Alghamdi, "Computerised Information Security Using Texture Based Fuzzy Cryptosystem," *Engineering, Technology & Applied Science Research*, vol. 8, no. 6, pp. 3598–3602, Dec. 2018, https://doi.org/10.48084/etasr.2353.

[23] L. Delamaire, H. A. H. Abdou, and J. Pointon, "Credit card fraud and detection techniques : a review," *Banks and Bank Systems*, vol. 4, no. 2, pp. 57–68, Jul. 2009.

[24] S. Bagga, A. Goyal, N. Gupta, and A. Goyal, "Credit Card Fraud Detection using Pipeling and Ensemble Learning," *Procedia Computer Science*, vol. 173, pp. 104–112, Jan. 2020, https://doi.org/10.1016/j.procs.2020.06.014.

[25] V. H. Le, N. Q. Luc, T. T. Dao, and Q. T. Do, "Building an Application that reads Secure Information Stored on the Chip of the Citizen Identity Card in Vietnam," *Engineering, Technology & Applied Science Research*, vol. 13, no. 1, pp. 10100–10107, Feb. 2023, https://doi.org/10.48084/etasr.5531.

[26] P. Save, P. Tiwarekar, K. N., and N. Mahyavanshi, "A Novel Idea for Credit Card Fraud Detection using Decision Tree," *International Journal of Computer Applications*, vol. 161, no. 13, pp. 6–9, Mar. 2017, https://doi.org/10.5120/ijca2017913413.

[27] J. Vimala Devi and K. S. Kavitha, "Fraud Detection in Credit Card Transactions by using Classification Algorithms," in *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, Mysore, India, Sep. 2017, pp. 125–131, https://doi.org/10.1109/CTCEEC.2017.8455091.

[28] B. Wickramanayake, D. K. Geeganage, C. Ouyang, and Y. Xu, "A Survey of Online Card Payment Fraud Detection using Data Mining-based Methods." arXiv, Nov. 27, 2020, https://doi.org/10.48550/arXiv.2011.14024.

[29] K. Modi and R. Dayma, "Review on fraud detection methods in credit card transactions," in *2017 International Conference on Intelligent Computing and Control (I2C2)*, Coimbatore, India, Jun. 2017, pp. 1–5, https://doi.org/10.1109/I2C2.2017.8321781.

[30] V. K. Prasad, "Method and system for detecting fraud in credit card transaction," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 5, 2013.

[31] S. Yadav and S. Siddartha, "Fraud Detection of Credit Card by Using HMM Model," *IMPACT: International Journal of Research in Engineering & Technology*, vol. 6, no. 1, Jan. 2018.

[32] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random forest for credit card fraud detection," in *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, Zhuhai, China, Mar. 2018, pp. 1–6, https://doi.org/10.1109/ICNSC.2018.8361343.

[33] H. Hormozi, M. K. Akbari, E. Hormozi, and M. S. Javan, "Credit cards fraud detection by negative selection algorithm on hadoop (To reduce the training time)," in *The 5th Conference on Information and Knowledge Technology*, Shiraz, Iran, Feb. 2013, pp. 40–43, https://doi.org/10.1109/IKT.2013.6620035.

[34] R. R. Popat and J. Chaudhary, "A Survey on Credit Card Fraud Detection Using Machine Learning," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, Feb. 2018, pp. 1120–1125, https://doi.org/10.1109/ICOEI.2018.8553963.

[35] W. Lovo, "Detecting credit card fraud: An analysis of fraud detection techniques," BSc Thesis, James Madison University, Harrisonburg, VA, USA, 2020.

[36] S. Mittal and S. Tyagi, "Performance Evaluation of Machine Learning Algorithms for Credit Card Fraud Detection," in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, Jan. 2019, pp. 320–324, https://doi.org/10.1109/CONFLUENCE.2019.8776925.

[37] A. Fawzi, S.-M. Moosavi-Dezfooli, and P. Frossard, "The Robustness of Deep Networks: A Geometrical Perspective," *IEEE Signal Processing Magazine*, vol. 34, no. 6, pp. 50–62, Aug. 2017, https://doi.org/10.1109/MSP.2017.2740965.

[38] D. K. M, V. Chadda, and H. Jain, "Credit Card Fraud Detection," *International Journal of Advanced Science and Technology*, vol. 29, no. 06, pp. 2201–2215, May 2020.

[39] I. Sadgali, N. Sael, and F. Benabbou, "Fraud detection in credit card transaction using neural networks," in *Proceedings of the 4th International Conference on Smart City Applications*, New York, NY, USA, Jul. 2019, pp. 1–4, https://doi.org/10.1145/3368756.3369082.

[40] A. Ali *et al.*, "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Applied Sciences*, vol. 12, no. 19, Jan. 2022, Art. no. 9637, https://doi.org/10.3390/app12199637.

[41] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Extraction of Common Concepts for the Mobile Forensics Domain," in *Recent Trends*

in Information and Communication Technology, Johor Bahru, Malaysia, 2018, pp. 141–154, https://doi.org/10.1007/978-3-319-59427-9_16.

[42] A. Ali, S. A. Razak, S. H. Othman, A. Mohammed, and F. Saeed, "A metamodel for mobile forensics investigation domain," *PLOS ONE*, vol. 12, no. 4, 2017, Art. no. e0176223, https://doi.org/10.1371/journal.pone.0176223.

[43] A. Al-Dhaqm *et al.*, "Categorization and Organization of Database Forensic Investigation Processes," *IEEE Access*, vol. 8, pp. 112846–112858, 2020, https://doi.org/10.1109/ACCESS.2020.3000747.

[44] "International Journal of Scientific Research in Computer Science, Engineering and Information Technology," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3, no. 5, pp. 320–325, 2018.

[45] P. R. Vardhani, Y. I. Priyadarshini, and Y. Narasimhulu, "CNN Data Mining Algorithm for Detecting Credit Card Fraud," in *Soft Computing and Medical Bioinformatics*, N. B. Muppalaneni, M. Ma, and S. Gurumoorthy, Eds. Singapore: Springer, 2019, pp. 85–93.

[46] R. J. Bolton and D. J. Hall, "Unsupervised Profiling Methods for Fraud Detection," Imperial College, London, UK.