International Journal of Economics, Management and Accounting

ISSN: 2988-7615 | 2023(5)
Page **391-398**

Research Article

Risky Mezi Muria

Fraud Detection Credit Card: A Bibliometric Analysis Approach

*Corresponding Author: **Risky Mezi Muria:** Universitas Trunojoyo Madura, Jawa Timur, Indonesia; ria.muria97@gmail.com

Received: October 15, 2023; **Accepted:** October 18, 2023; **Online:** October 21, 2023. | DOI: https://doi.org/10.47353/ijema.v1i5.69

Abstract: *The aim of this research is to provide research possibilities for future research. This research uses bibliometrics. Samples of journals or articles after going through a selection process with purposive sampling of 50 journals or articles from 2017-2021. Data sources come from journals and articles published in Science Direct, Emerald Insight and Google Scholar. The results of this research are that Google Scholar is the source of the most popular journals or articles and IEEE is the largest publication in credit card fraud detection publications. Opportunities for further research could be to apply some of the proposed new methods to various types of credit card fraud data.*

Keywords*: fraud, credit card, fraud detection.*

Introduction

Rapid economic development and the presence of online buying and selling transactions have an impact on consumer behavior in transactions. One method used in financial transactions is a credit card (Hendarsyah, 2020). From data released by Bank Indonesia in 2021, the use of credit cards in circulation as of October 2021 was 16,545,925. Meanwhile, credit card transactions from Bank Indonesia data until October 2021 were 24,764,344 transactions with a value of 21,428,798,000,000. This is because electronic payment systems such as credit cards are faster, more flexible and without having to go to the bank (Wulandari, 2019).

In Indonesia, credit card fraud is in the second lowest position compared to other countries in the Asia Pacific region. Meanwhile, based on Visa data, ranking *fraud* Indonesia is in the third lowest position compared to other countries in Southeast Asia (Sulisrudatin, 2018). Even though credit cards provide many conveniences as an electronic means of payment, on the other hand, credit cards can be a crime whether in terms of procurement or other forms of crime. The practice of misuse of credit cards often occurs either through criminal (default) or technological crimes in various forms (carding or card fraud). (Wulandari, 2019).

The carding perpetrator obtained the victim's credit card data illegally (illegal interception) and then used the credit card to shop at an online shop (forgery) (Sulisrudatin, 2018). This method may occur due to a weak authentication system used to ensure the identity of the orderer of goods in an online shop. Apart from carding cases, there are also cases related to credit cards, namely credit card identity theft (fraud). The motive for this crime is considered to be work factors and the opportunity or chance to trick the victim into being willing to give him his credit card (Shirodkar et al., 2020).

Thus, there is a need to increase security in processing credit card transactions. To minimize the occurrence of credit card fraud, detection and prevention is necessary. Research fromSitohang et al., (2021)explained that detecting fraud patterns using Modified ADASYN for credit card transactions requires good accuracy, this is because the better the detection accuracy, the smaller the losses caused by fraudulent transactions. Another method for detecting credit card fraud in researchYazid & Fiananta, (2017) explained

that the use of data mining can help to detect fraud that occurs by recognizing transaction patterns (patterns), one of the popular data mining is support vector machine (SVM).

The aim of this research is to provide an overview of the development of big data research in the financial sector and provide several research opportunities that can be followed up by future researchers. The contribution of this research is to add to the literature on the development of credit card fraud detection research and provide an overview of future research opportunities.

Fraud is a process of using one's responsibilities to satisfy one's personal interests by enriching oneself through deliberate abuse of power (ACFE, 2017). Financial and Development Supervisory Agency, (2008)explained "Fraud is an act against or breaking the law committed by people from inside or outside the organization, with the intention of gaining personal or group benefits directly or indirectly to the detriment of other parties. While Webster's New World Dictionary in(Financial and Development Supervisory Agency, 2008). Fraud is a general terminology, which includes various meanings regarding ingenuity, trickery, human deception used by someone, to gain an advantage (over) another person through misrepresentation. There are no standard and definite rules that can be used as more words to give another meaning about fraud, except how to carry out deception, unnaturally and cleverly so that other people are deceived. The only thing that can be a limitation regarding fraud is that it is usually carried out by those who are dishonest/full of deceit.

In general, fraud can be defined as a general term, and includes all kinds of methods that can be used with particular skill, chosen by an individual, to obtain benefits from other parties by making false representations (Sudarmanto, 2020). The occurrence of fraud in corporate organizations can originate from internal and external sources (Sudarmanto, 2020) explains the internal sources that trigger fraud in corporate organizations, namely corruption, presentation of false reports, fabricated financial reports, duplicate financial reports, theft or inappropriate use of organizational assets by employees and management to fulfill personal or group interests and inappropriate use. not in accordance with its intended purpose, while external sources trigger fraud such as bribery, inflating the value of invoices, double invoices and quality fraud such as goods transactions that do not conform to the agreed presentation. (Sayyid, 2015).

The way to detect credit card fraud is by supervised techniques that rely on a collection of past transactions for which the labels (also referred to as outcomes or classes) of those transactions are known. In the case of credit card fraud detection, the labels are genuine (transactions made by the cardholder) or fraudulent (transactions made by fraudsters). These labels are usually identified a posteriori, either due to customer complaints or as a result of an investigation by the credit card company. Supervised techniques utilize labeled past transactions to learn a fraud prediction model, which returns, for each new transaction, the probability of it being fraudulent. However, not all labels are available immediately (Carcillo et al., 2021)

Credit cards are a very popular payment method and are widely used in online transactions (Yazid & Fiananta, 2017). According to (Fayyomi et al., 2021) Credit cards are an electronic payment method. Credit cards are thin rectangular pieces of plastic or metal issued by banks or financial services companies to consumers (card holders) to facilitate payments to merchants of goods and services.

Fraud detection techniques such as statistical data analysis and artificial intelligence can be used to differentiate between the two. AI techniques include data mining used to detect fraud, which can classify, group, and segment data to search through millions of transactions to find patterns and detect fraud. Machine learning is a technique for automatically detecting the characteristics of fraud. One method of dealing with fraud is through prevention and detection. Fraud detection and prevention's primary goal is to differentiate between legitimate and fraudulent transactions and to prevent fraudulent activity. Using

historical data, user patterns and behavior are analyzed to determine whether a transaction is fraudulent or not. When systems fail to detect and prevent fraudulent activity, fraud detection takes over (Popat & Chaudhary, 2018).

According to Suryohadibroto and Prakoso in (Hendarsyah, 2020), a credit card is a means of payment as a substitute for cash which consumers can use at any time to exchange for the products and services they want at places that accept credit cards (merchants) or consumers can use it to cash out at the issuing bank or its network (cash advance). Credit card fraud is the misuse of credit card information to make purchases without authorization (ACFE, 2017). Credit card fraud works because the chances of being caught are small and prosecution is not guaranteed. The types of credit card schemes include selling cards to thieves, family members using credit cards without permission, and obtaining cards fraudulently (ACFE, 2017). Apart from that, credit card fraud (Vimala Devi & Kavitha, 2018) method:

a) Credit Card Fraud: credit card fraud, in general, is of two types: Offline and online fraud. Offline fraud can be carried out in many ways such as using stolen physical cards, scanning cards like real cards or duplicating electronic information from cards that are in any place. Since swiping a PIN or card imprint, online fraud is possible even remotely which can be carried out via the internet or telecommunications.
b) Phone call fraud: Phone calls can be used to commit other forms of fraud such as extracting card details from cardholders by impersonating bank authorities. In general, credit card holders, merchants and communications service providers are the main prey.
c) Computer Intrusion: The act of violating privacy without authorization or authentication is defined as Intrusion. By intentionally attempting to access and manipulate information in an unauthorized manner.
d) Fake card fraud: This is a white collar crime that focuses on creating fake cards that retain the details of fully functional real cards. This fraud is carried out through skimming.
e) CNP Fraud: This is referred to as Credit Not Present fraud. This kind of crime can be committed if the criminal knows the expiration date and account number for the card, without having the physical card.

Challenges of Credit Card Fraud Detection In previous work we conducted a systematic review of data mining approaches for credit card fraud detection and identified significant challenges in this area (Mekterović et al., 2021).

1) Lack of Data Lack of data can be considered in two contexts: lack of literature on the topic and lack of training/testing data (public credit card transaction databases). The latter is a problem for scientists and not so much for industry, because credit card processing houses have huge amounts of data. The first is often cited as a problem, but we respectfully disagree because there are many people on the topic and even books. It can be surmised that there is the opposite problem—surveying and assimilating a large and scattered literature to discern best practices and methodologies.
2) Feature Engineering Feature engineering is a classic topic in data mining and is very important in credit card fraud detection. Credit card processing companies and banks typically have a rich set of features on credit card holders that can be used to build user/card profiles, especially when enriched with values accumulated from previous card transactions that reflect the card profile. An interesting exception is a system where the main means of payment is a prepaid card that is not associated with a person. Prepaid cards are rarely loaded with money. Card lifetimes are relatively short—from months to a year, for example. Therefore, there is a limited set of features available and little information for modeling the cards. Such a system is described in and in predicting card fraud, the authors use a dozen features as opposed to the several hundred we use in our simulations.
3) Scalability Scalability is a technical issue that is often overlooked in the literature. One must strive to design a robust and scalable system to maintain a large and continuous flow of transactions.

4) Concept Drift Credit card fraud patterns change over time as markets and technology change, and both fraudsters and card processors adapt to these changes. This changes the underlying patterns and data and is referred to as “concept drift”. Predictive models operating in these settings need to have mechanisms to: (i) detect concept drift and adapt if necessary; and (ii) distinguishes deviation from noise and is adaptive to change, but robust to noise. Simply put, models become stale and outdated and must be refreshed or evolved. The existing concept drift detection techniques are window-based, orensemble-based statistics. Readers interested in adapting prediction models to the concept of drift (i.e., adaptive learning) are referred to in recent reviews and the most cited reviews deal with the concept of drift.
5) Performance Measures As is often quoted, “What cannot be measured cannot be improved”, so it is important to determine the right metrics for our models. There are a large number of metrics proposed in the literature, and in our work we propose a simple and informative chart to compare competing models. Fraud detection is usually defined as a classification task: transactions are classified as fraudulent or non-fraudulent. In our opinion, this should be considered from a detection perspective: a set of transactions are ranked based on their likelihood of fraud, which maps very well to the business case. Since transactions must ultimately be reviewed by human experts, it is useful to rank them according to probability of fraud. One can determine a “fraud threshold”, for example, with a probability of 50%. Still, that's irrelevant: a finite number of human experts in a finite amount of time will only be able to analyze a finite number of transactions, and they must do so in order of fraud probability. Credit card processors can trade fraud losses against analyst fees and achieve an optimal balance.
6) Algorithm Model Selection Finally, many different data mining algorithms can address this problem. Each of them presents an optimization problem with many hyperparameters to tune. Then they can be combined to form ensembles and so on. It is impossible to “try them all”, so for practical reasons, the “best” algorithm or a short list of algorithms should be selected at the first step of investing resources.

Method

This research uses a bibliometric approach based on science mapping analysis and performance indicators used with the aim of revealing the status of credit card fraud detection research. This research will map out (1) Number of Journals (2) Type of research, (3) Publication, (4) Type detection used. Data sources come from journals and articles published in Science Direct, Emerald Insight and Google Scholar. The search engines used were "credit card fraud detection", "credit card fraud detection", "credit card fraud detection", and "credit card service fraud detection". The year range used is 2016-2021.

Results and Discussion

The first finding in this research is the trend in the number of articles published in the Google Scholar database during the period 2017 to 2021. Based on data obtained from the Google Scholar database, articles related to credit card fraud detection after going through the selection process with purposive sampling are 50 journals or article. Based on Figure 1, the number of journals or articles from IEEE is 24, Science Direct (SD) is 3 journals or articles, Springer is 5 journals, Research Gate is 7 journals or articles.

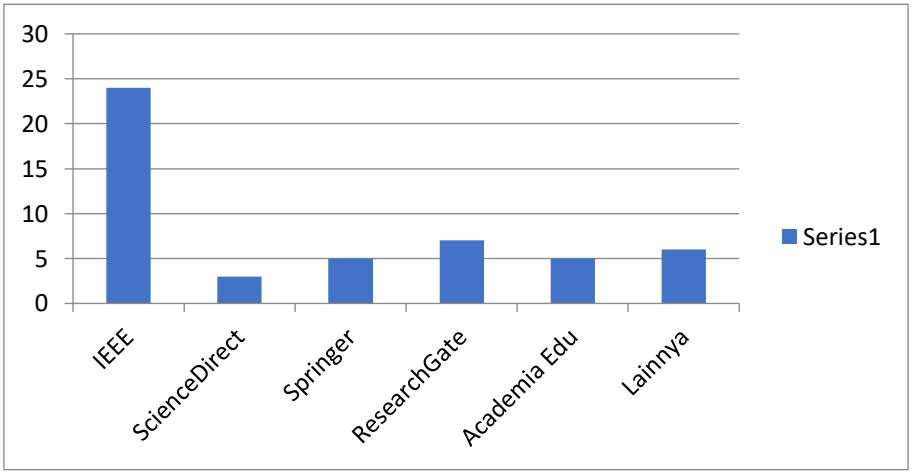

Image: Number of Journals published in Google Scholar
Source: Processed by researchers

This research also classifies articles based on the type of research approach used by each article which is shown in Figure 2. Based on the results of the analysis of 50 articles, the quantitative approach is the approach most widely used by researchers in discussing credit card fraud detection, namely 33 articles and that the most used in 2018 was 10 articles. Furthermore, the mixed method approach was 10 articles and the most widely used in 2020 was 6 articles and the qualitative approach was 2 articles in 2017 and 2019 and the experimental approach was the same amount, namely 2 articles, but only in 2019. Meanwhile, the survey approach is in last place, namely 1 article in 2017. The method most widely used in the quantitative approach is the use of system-related fraud detection methods.

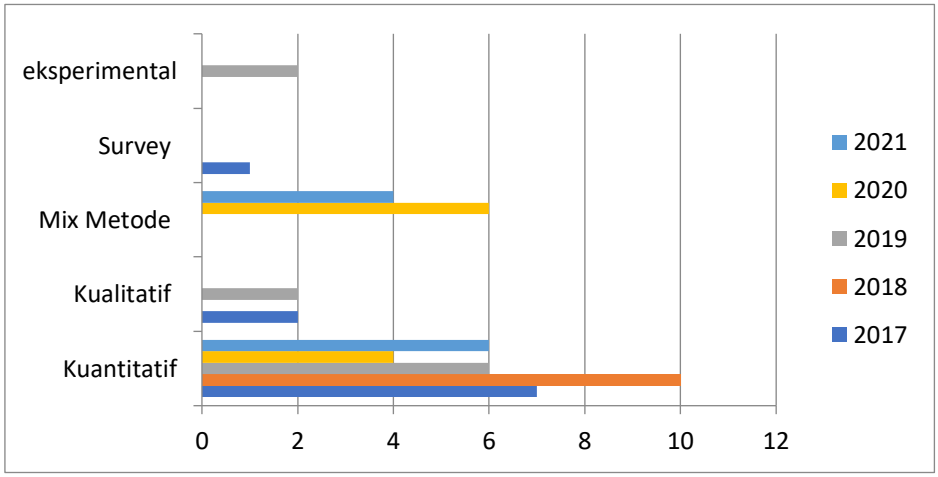

Image: classification of articles based on type of research approach
Source: Processed by researchers

Apart from that, there is still a lack of research regarding disclosing the causes of credit card fraud so that researchers have several limitations in conducting empirical research. However, this can be overcome by carrying out more research experiments. From the data obtained, the experiment was carried out only twice from 2017-2021. If research detects fraud on credit cards using experiments, the data will cover existing limitations.

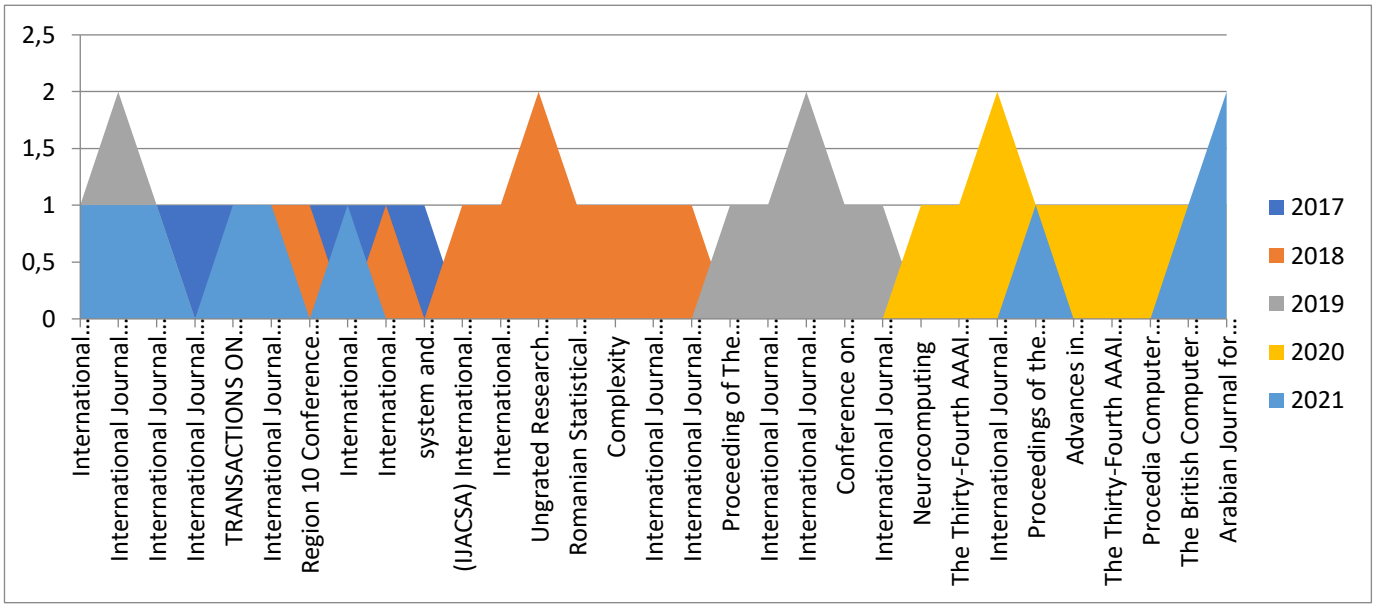

Image: Publication Statistics
Source: Data processed by researchers

Based on Figure 3, it is explained which publications publish journals or articles. Arabian Journal for Science and Engineering by contributing 3 journals in 2017-2021. International Conference on Computational Intelligence and Computing Research contributed 3 journals, International Journal of Computer Science and Business Informatics contributed 4 journals, International Journal of Computer Networking and Informatics 3 journals, International Journal of Engineering Research & Technology (Ijert) 1 journal, Transactions On Neural Networks And Learning Systems 1 journal and the rest all publications contributed 1-2 journals from 2017-2021. By looking at the source of this publication, it proves that the journals used as samples are quality journals or articles. Apart from that, it can provide references for future researchers.

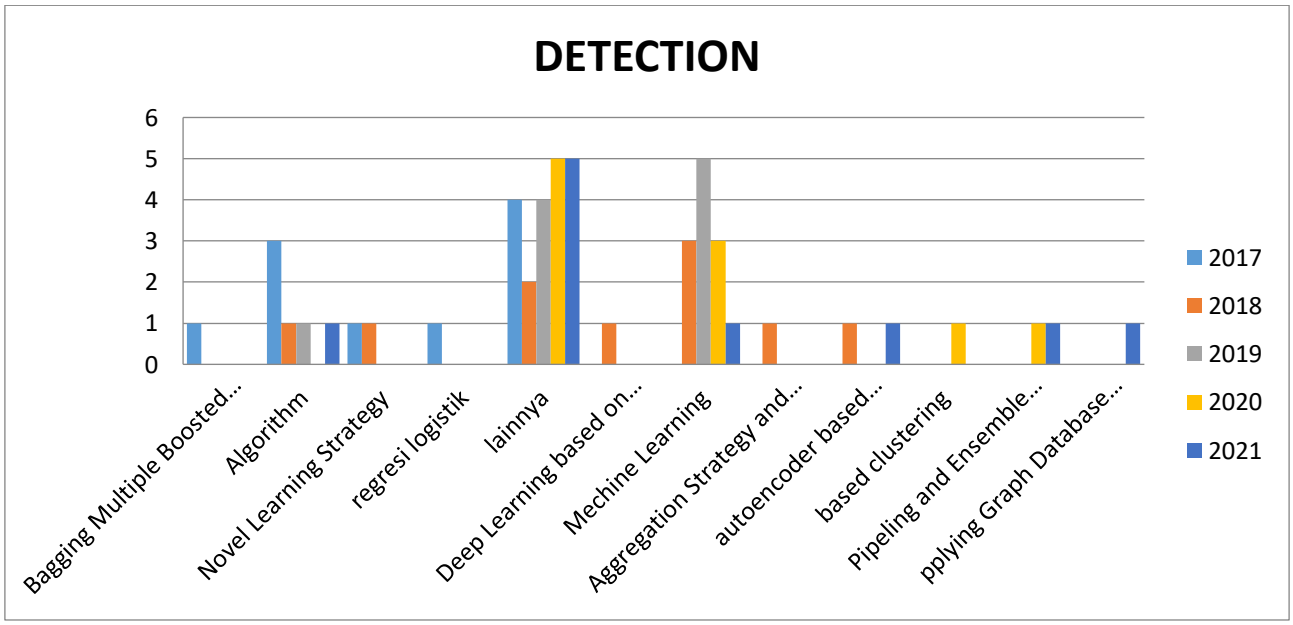

Image: Credit Card Fraud Detection
Source: Processed by researchers

Based on Figure 4, the detection of credit card fraud uses various detection methods carried out by researchers from 2017-2021. Research results from 2017-2021 show that detecting credit card fraud using the Bagging Multiple Boosted Trees (BMBT) method is 1,*Algorithm*6, Novel Learning Strategy 2, logistic regression 1, others 20 including research using experiments, Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine 1, Machine Learning 12, Aggregation Strategy and Feedback Mechanism 1, 2 autoencoder based clustering, 1 based clustering, 2 Pipeling and Ensemble Learning, and 1 research journal pplying Graph Database Model.

Based on Figure 4, the detection of credit card fraud involves analyzing big data based on data type, data source, type of fraud and methods, namely algorithms and machine learning. The results of the proposed study show that claim anomalies detected using this application enable credit card fraud to be detected as early as possible. Potential benefits of big data analytics include detecting credit card fraud more quickly and efficiently.

Conclusion

Based on the results of research that has carried out mapping and analysis of the 50 journals or articles used. Google Scholar is the largest source of journals or articles. The most frequently conducted research is qualitative research. IEEE is the largest publication in credit card fraud detection publications. Opportunities for further research could be to apply some of the proposed new methods to various types of credit card fraud data.

References

ACFE. (2017). Fraud Examiners Manual.

Badan Pengawasan Keuangan dan Pembangunan. (2008). Pusdiklatwas BPKP.

Carcillo, F., Le Borgne, Y. A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. Information Sciences, 557(xxxx), 317–331. https://doi.org/10.1016/j.ins.2019.05.042

Fayyomi, A. M., Eleyan, D., & Eleyan, A. (2021). A Survey Paper On Credit Card Fraud Detection Techniques. October.

Hendarsyah, D. (2020). Analisis Perilaku Konsumen Dan Keamanan Kartu Kredit Perbankan. JPS (Jurnal Perbankan Syariah), 1(1), 85–96. https://doi.org/10.46367/jps.v1i1.204

Mekterović, I., Karan, M., Pintar, D., & Brkić, L. (2021). Credit card fraud detection in card-not-present transactions: Where to invest? Applied Sciences (Switzerland), 11(15). https://doi.org/10.3390/app11156766

Popat, R. R., & Chaudhary, J. (2018). A Survey on Credit Card Fraud Detection Using Machine Learning. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018, Icoei, 1120–1125. https://doi.org/10.1109/ICOEI.2018.8553963

Sayyid, A. (2015). Pemeriksaan Fraud Dalam Akuntansi Forensik Dan Audit Investigatif. Al-Banjari : Jurnal Ilmiah Ilmu-Ilmu Keislaman, 13(2), 137–162. https://doi.org/10.18592/al-banjari.v13i2.395

Shirodkar, N., Mandrekar, P., Mandrekar, R. S., Sakhalkar, R., Chaman Kumar, K. M., & Aswale, S. (2020). Credit Card Fraud Detection Techniques - A Survey. International Conference on Emerging Trends in Information Technology and Engineering, Ic-ETITE 2020, 1–7. https://doi.org/10.1109/ic-ETITE47903.2020.112

Sitohang, E. H., Setiabudi, D. H., & Ananda, S. A. (2021). Penerapan Modified ADASYN untuk Meningkatkan Akurasi Pendeteksian Pola Fraud pada Transaksi Kartu Kredit. Jurnal Infra, 0–6.

Sudarmanto, E. (2020). Manajemen Risiko: Deteksi Dini Upaya Pencegahan Fraud. Jurnal Ilmu Manajemen, 9(2), 107. https://doi.org/10.32502/jimn.v9i2.2506

Sulisrudatin, N. (2018). ANALISA KASUS CYBERCRIME BIDANG PERBANKAN. 9(1), 26–39.

Vimala Devi, J., & Kavitha, K. S. (2018). Fraud Detection in Credit Card Transactions by using Classification Algorithms. International Conference on Current Trends in Computer, Electrical, Electronics and Communication, CTCEEC 2017, 125–131. https://doi.org/10.1109/CTCEEC.2017.8455091

Wulandari, S. (2019). PERLINDUNGAN HUKUM BAGI NASABAH PERBANKAN TERHADAP KEJAHATAN KARTU KREDIT. 17(0854), 29–38.

Yazid, Y., & Fiananta, A. (2017). Mendeteksi Kecurangan Pada Transaksi Kartu Kredit Untuk Verifikasi Transaksi Menggunakan Metode Svm. Indonesian Journal of Applied Informatics, 1(2), 61–66.