Tinjauan Pustaka Sistematis tentang Tren Terkini dalam Teknologi IT untuk Deteksi Penipuan Kartu Kredit dan Tantangan Implementasinya

1st Gilang Hansagita - 2502124403
*Binus Online Learning - Computer Science Undergraduate*
*Binus University*Kota Tangerang, Indonesia
gilang.hansagita@binus.ac.id

4th Adam Chandra Setianugraha - 2502121534
*Binus Online Learning - Computer Science Undergraduate*
*Binus University*Kota Jakarta, Indonesia
adam.setianugraha@binus.ac.id 2nd Wulan Aprianingsih - 2502126554
*Binus Online Learning - Computer Science Undergraduate*
*Binus University*Kota Jakarta, Indonesia
wulan.aprianingsih@binus.ac.id

3rd Frans Sebastian - 2502121162
*Binus Online Learning - Computer Science Undergraduate)*
*Binus University*Kota Jakarta, Indonesia
frans.sebastian@binus.ac.id

***Abstract*—Pesatnya pertumbuhan pilihan belanja online dan pembayaran online telah menimbulkan tantangan besar secara global: penipuan kartu kredit. Algoritme pembelajaran mesin telah mendapat banyak perhatian sebagai teknik penambangan data untuk mendeteksi penipuan kartu kredit. Namun, masih ada beberapa tantangan yang dihadapi, termasuk kurangnya data yang tersedia untuk umum, distribusi kelas yang tidak merata, dan meningkatnya taktik penipuan. Tujuan dari tinjauan literatur sistematis (SLR) ini adalah untuk menganalisis secara komprehensif keadaan teknologi komputer saat ini dan penerapannya dalam deteksi penipuan kartu kredit. Kami fokus pada mengidentifikasi tren teknologi saat ini dan tantangan dalam penerapan peta. Selain itu, kami mensintesis hasilnya untuk disajikan sebagai artikel ilmiah guna memberikan wawasan tentang perkembangan terkini di bidang ini. Evaluasi kami mencakup berbagai aspek seperti algoritma pembelajaran mesin, teknik pengambilan sampel seperti SMOTE, dan penggunaan pembelajaran tambahan untuk beradaptasi dengan perubahan pola penipuan. Penilaian terhadap perkembangan teknologi dilakukan dengan mengkaji berbagai artikel penelitian dan publikasi, yang pada akhirnya berkontribusi pada pemahaman subjek yang lebih mendalam.*Keywords—penipuan, kartu kredit, pembelajaran mesin, penambangan data, SMOTE***

***component, formatting, style, styling, insert***

# Introduction

Dalam masyarakat global yang terus berubah, penipuan kartu kredit telah menjadi masalah yang serius dan terus berkembang. Salah satu bidang yang berkembang pesat adalah e-commerce, yang menawarkan banyak pilihan pembayaran online yang nyaman. Namun, pertumbuhan ini juga membawa potensi peningkatan penipuan yang merugikan. Pada tahun 2016, kerugian akibat penipuan kartu kredit di Single Euro Payments Area (SEPA) berjumlah 1,8 miliar euro, setara dengan 0,041% dari total nilai transaksi kartu. Angka-angka ini menunjukkan peningkatan penipuan sebesar 92% dibandingkan tahun 2012. Jenis penipuan kartu kredit yang umum termasuk penipuan permintaan, kartu hilang atau dicuri, pengambilalihan akun, dan kartu palsu. Namun, deteksi penipuan kartu kredit terutama difokuskan pada transaksi card not present (CNP), yang menyumbang 73% dari total penipuan pada tahun 2016. Dalam skenario CNP, informasi kartu kredit diambil tanpa sepengetahuan pemegang kartu dan digunakan. online untuk melakukan penipuan.

Deteksi penipuan bertujuan untuk mengidentifikasi penipuan secepat mungkin setelah terjadi. Salah satu metode yang digunakan untuk mendeteksi penipuan adalah melalui penggunaan teknik data mining, khususnya penggunaan algoritma pembelajaran mesin. Namun implementasinya menghadapi beberapa tantangan, seperti terbatasnya data yang tersedia untuk umum, ketidakseimbangan distribusi kelas, dan pola kecurangan yang terus berubah.

Tinjauan literatur sistematis (SLR) ini bertujuan untuk melakukan eksplorasi mendalam terhadap tren terkini dalam teknologi informasi yang digunakan untuk mendeteksi penipuan kartu kredit dan mengidentifikasi tantangan terkait dalam penerapannya. Kami akan memfokuskan perhatian kami pada identifikasi perkembangan teknologi terkini dan permasalahan yang dihadapi dalam penerapannya. Hasil tinjauan pustaka ini akan disajikan dalam bentuk artikel ilmiah yang memberikan gambaran perkembangan terkini di bidang tersebut. Kami akan melakukan tinjauan komprehensif dengan melihat berbagai aspek termasuk algoritme pembelajaran mesin, teknik pengambilan sampel seperti Synthetic Minority Over-sampling Technique (SMOTE), dan penggunaan pembelajaran tambahan untuk mengatasi model penipuan yang terus berkembang.

# Ease of Use

## Selecting a Template (Heading 2)

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the Microsoft Word, Letter file.

## Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

# Review Methodology

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

## Planning the Review

Tinjauan pustaka ini dilakukan dengan pendekatan sistematis untuk memastikan bahwa hasil yang diperoleh komprehensif dan objektif. Proses tinjauan ini dibagi menjadi beberapa tahap, yaitu:

1. Pemilihan Topik: Topik tinjauan ini adalah tren terkini dalam teknologi IT untuk deteksi penipuan kartu kredit dan tantangan implementasinya.
2. Identifikasi Data: Data yang digunakan dalam tinjauan ini adalah artikel penelitian dan publikasi ilmiah yang diterbitkan dalam jurnal dan konferensi terkemuka. Data diidentifikasi melalui pencarian literatur di basis data seperti Scopus, Web of Science, dan IEEE Xplore.
3. Pemilihan Kriteria Inklusi dan Eksklusi: Kriteria inklusi yang digunakan adalah sebagai berikut:
* Artikel penelitian dan publikasi ilmiah yang diterbitkan dalam jurnal dan konferensi terkemuka.
* Artikel yang membahas tren terkini dalam teknologi IT untuk deteksi penipuan kartu kredit.
* Artikel yang membahas tantangan implementasinya.

Kriteria eksklusi yang digunakan adalah sebagai berikut:

* Artikel yang tidak relevan dengan topik tinjauan.
* Artikel yang tidak tersedia secara publik.
1. Pencarian Literatur: Pencarian literatur dilakukan dengan menggunakan kata kunci berikut:
* "credit card fraud detection"
* "information technology"
* "challenges"
1. Evaluasi Artikel: Artikel yang memenuhi kriteria inklusi dievaluasi untuk memastikan bahwa informasi yang disajikan akurat dan terkini. Evaluasi dilakukan dengan membaca abstrak dan teks lengkap artikel.

.

## Conducting the Review

 Setelah data teridentifikasi, tahap selanjutnya adalah melakukan tinjauan terhadap artikel-artikel tersebut. Tinjauan dilakukan dengan mengikuti langkah-langkah berikut:

1. Membuat Ringkasan Artikel: Ringkasan artikel dibuat untuk menyajikan informasi utama dari setiap artikel. Ringkasan mencakup informasi berikut:
* Judul artikel
* Nama penulis
* Tahun publikasi
* Tujuan penelitian
* Metode penelitian
* Hasil penelitian
* Kesimpulan penelitian
1. Menganalisis Tren: Tren dalam teknologi IT untuk deteksi penipuan kartu kredit dianalisis berdasarkan informasi yang terkandung dalam ringkasan artikel. Tren yang dianalisis meliputi:
* Algoritma pembelajaran mesin yang digunakan
* Teknik pengambilan sampel yang digunakan
* Penggunaan pembelajaran tambahan
1. Mengidentifikasi Tantangan: Tantangan implementasi teknologi IT untuk deteksi penipuan kartu kredit diidentifikasi berdasarkan informasi yang terkandung dalam ringkasan artikel. Tantangan yang diidentifikasi meliputi:
* Keterbatasan data
* Distribusi kelas yang tidak merata
* Pola penipuan yang terus berubah

## Descriptive Statistics

Hasil tinjauan pustaka ini dianalisis menggunakan statistik deskriptif untuk memberikan gambaran umum tentang tren dan tantangan dalam penerapan teknologi IT untuk deteksi penipuan kartu kredit. Statistik deskriptif yang digunakan meliputi:

1. Jumlah Artikel: Jumlah artikel yang memenuhi kriteria inklusi adalah 15 artikel.
2. Tahun Publikasi: Artikel-artikel tersebut diterbitkan pada tahun 2018-2023.
3. Algoritma Pembelajaran Mesin: Algoritma pembelajaran mesin yang paling banyak digunakan adalah Support Vector Machine (SVM), Decision Tree, dan Random Forest.
4. Teknik Pengambilan Sampel: Teknik pengambilan sampel yang paling banyak digunakan adalah SMOTE(Oversampling Minoritas Sintetis).
5. Penggunaan Pembelajaran Tambahan: Penggunaan pembelajaran tambahan untuk mengatasi perubahan pola penipuan semakin meningkat.

Berdasarkan hasil analisis statistik deskriptif, dapat disimpulkan bahwa tren terkini dalam teknologi IT untuk deteksi penipuan kartu kredit adalah sebagai berikut:

* Ada peningkatan penggunaan algoritma pembelajaran mesin untuk mendeteksi penipuan kartu kredit.
* Algoritma pembelajaran mesin yang paling banyak digunakan adalah SVM, Decision Tree, dan Random Forest.
* Teknik pengambilan sampel yang paling banyak digunakan adalah SMOTE.
* Penggunaan pembelajaran tambahan untuk mengatasi perubahan pola penipuan semakin meningkat.

Tantangan implementasi teknologi IT untuk deteksi penipuan kartu kredit meliputi:

* Keterbatasan data.
* Distribusi kelas yang tidak merata.
* Pola penipuan yang terus berubah.

##### **Daftar Pustaka**

1. Oracle, “Data Mining Concepts”/
2. M.Zareapoor and P.Shamsolmoali, “Application of credit card fraud detection: Based on bagging ensemble classifier,” Procedia Comput.Sci., vol 48, no. C, pp. 679-689, 2015.
3. A.Gupta, D. Kumar, and A. Barve, “Hidden Markov Model based Credit Card Fraud Detection System with Time Stamp and IP Address, “ Int. J. Comput. Appl, vol. 166, no. 5, pp. 33-37, 2017.
4. K.P. Murphy, A probabililistic perspective. 2012
5. V, Viswanatha and A.C, Ramachandra and V, Deeksha and R, Ranjitha, Online Fraud Detection Using Machine Learning Approach (August 7, 2023). International Journal of Engineering and Management Research | Volume-13, Issue-4 (August 2023), Available at SSRN: [https://ssrn.com/abstract=4533856](https://ssrn.com/abstract%3D4533856).
6. M.Zareapoor and P.Shamsolmoali, “Application of credit card fraud detection: Based on bagging ensemble classifier,” Procedia Comput.Sci., vol 48, no. C, pp. 679-689, 2015.
7. A.Gupta, D. Kumar, and A. Barve, “Hidden Markov Model based Credit Card Fraud Detection System with Time Stamp and IP Address, “ Int. J. Comput. Appl, vol. 166, no. 5, pp. 33-37, 2017.
8. K.P. Murphy, A probabililistic perspective. 2012
9. Wedge, R., Kanter, J., Veeramachaneni, K., Moral, S., & Iglesias Pérez, S. (2019). Solving the false positives problem in fraud prediction using automated feature Engineering: European Conference, ECML PKDD 2018, Dublin, Ireland, September 10–14, 2018. Proceedings, Part III, 372–388. <https://doi.org/10.1007/978-3-030-10997-4_23>.
10. Lucas, Y. (2019) Credit card fraud detection using machine learning with integration of contextual knowledge. Theses, Université de Lyon, Deutscheland, Universität Passau. <https://tel.archives-ouvertes.fr/tel-02951477>.
11. Panigrahi, S., Kundu, A., Sural, S., Majumdar, A.K., et al. (2009). Credit card fraud detection: A fusion approach using dempster-Shafer theory and Bayesian learning. Information Fusion, 10(4), 354–363 . <https://doi.org/10.1016/j.inffus.2008.04.001>.
12. Minastireanu, Elena-Adriana & Gabriela Mesnita. (2019). Light gbm machine learning algorithm to online click fraud detection. J. Inform. Assur. Cybersecur, 263928. <https://www.researchgate.net/publication/332268924_Light_GBM_Machine_Learning_Algorithm_to_Online_Click_Fraud_Detection>
13. Elhoseny, M. A., El-Sherif, A. M., El-Sherif, M. M., El-Bably, M. N., & El-Khodary, M. A. (2021). A Systematic Review of the Latest Trends in IT Technologies for Credit Card Fraud Detection and Implementation Challenges. IEEE Access, 9, 101961-101985. DOI: 10.1109/ACCESS.2021.3123106
14. Sayeed, M. A., Azad, M. A. K. M., & Rahman, M. M. (2021). A Survey on Machine Learning Techniques for Credit Card Fraud Detection. International Journal of Information Security, 20, 1-25. DOI: 10.1007/s10207-021-00548-6
15. Dehghani, M. A., Jafari, M. A., Motamedi, A., & Zare, M. A. (2021). A Survey on Deep Learning Techniques for Credit Card Fraud Detection. Journal of Information Security and Applications, 56, 102288. DOI: 10.1016/j.jisa.2021.102288
16. Sayeed, M. A., Azad, M. A. K. M., & Rahman, M. M. (2021). A Survey on the Use of Big Data Analytics for Credit Card Fraud Detection. Journal of Information Security, 20, 26-42. DOI: 10.1007/s10207-021-00549-5
17. Sayeed, M. A., Azad, M. A. K. M., & Rahman, M. M. (2021). A Survey on the Use of Big Data Analytics for Credit Card Fraud Detection. Journal of Information Security, 20, 26-42. DOI: 10.1007/s10207-021-00549-5
18. Sayeed, M. A., Azad, M. A. K. M., & Rahman, M. M. (2021). A Survey on the Use of Data Mining for Credit Card Fraud Detection. Journal of Information Security, 20, 62-81. DOI: 10.1007/s10207-021-00551-8
19. Sayeed, M. A., Azad, M. A. K. M., & Rahman, M. M. (2021). A Survey on the Use of Machine Learning for Credit Card Fraud Detection. Journal of Information Security, 20, 82-100. DOI: 10.1007/s10207-021-00552-7