


PLAGIARISM SCAN REPORT

Date October 23, 2023

Exclude URL: NO

	Unique Content	100	Word Count	2188
	Plagiarized Content	0	Records Found	0

CONTENT CHECKED FOR PLAGIARISM:

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

XXX-X-XXXX-XXXX-X/XX/\$XX.00 ©20XX IEEE

1st Gilang Hansagita - 2502124403

Binus Online Learning - Computer Science Undergraduate

Binus University

Kota Jakarta, 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, penambahan data, SMOTE

I. 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.

II. Ease of Use

II.1. 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.

II.2. 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.

III. Review Methodology

III.1. 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.

4. Pencarian Literatur: Pencarian literatur dilakukan dengan menggunakan kata kunci berikut:

- * "credit card fraud detection"
- * "information technology"
- * "challenges"

5. 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.

.

III.2. 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

2. 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

3. 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

III.3. 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.

IV. Review findings and discussions

Analisis dan pembahasan hasil studi literatur berdasarkan rumusan masalah (research questions) yang telah dituliskan dalam review methodology dapat disajikan sebagai berikut:

Research Question 1: Bagaimana tren terkini dalam teknologi IT digunakan untuk mendeteksi penipuan kartu kredit?

Hasil tinjauan literatur menunjukkan bahwa teknologi IT telah mengalami perkembangan yang pesat dalam upaya mendeteksi penipuan kartu kredit. Algoritme pembelajaran mesin menjadi fokus utama dalam menghadapi tantangan ini. Banyak penelitian terbaru telah mengeksplorasi metode pembelajaran mesin seperti Random Forest, Neural Networks, dan Support Vector Machines untuk mengidentifikasi pola penipuan yang semakin kompleks. Selain itu, teknik pengolahan bahasa alami (NLP) juga mulai digunakan untuk menganalisis teks terkait transaksi dan perilaku pengguna.

Research Question 2: Apa saja tantangan utama dalam implementasi teknologi IT untuk deteksi penipuan kartu kredit?

Terdapat beberapa tantangan kunci dalam implementasi teknologi IT untuk deteksi penipuan kartu kredit. Pertama, terdapat masalah kurangnya data yang tersedia untuk umum, terutama data penipuan yang terbatas. Hal ini mempengaruhi kemampuan algoritme pembelajaran mesin untuk mengidentifikasi pola penipuan dengan akurasi yang tinggi. Selain itu, distribusi kelas yang tidak merata, di mana sebagian besar transaksi adalah transaksi yang sah, juga merupakan tantangan. Hal ini bisa mengakibatkan algoritme cenderung "mengabaikan" kasus penipuan. Di samping itu, para penipu terus mengembangkan taktik mereka, sehingga algoritme harus dapat beradaptasi dengan perubahan pola penipuan yang terus berkembang.

Research Question 3: Bagaimana teknologi IT dapat mengatasi tantangan yang dihadapi dalam deteksi penipuan kartu kredit?

Dalam upaya mengatasi tantangan dalam deteksi penipuan kartu kredit, beberapa teknik dan pendekatan telah diusulkan. Salah satu pendekatan yang umum digunakan adalah oversampling menggunakan metode seperti SMOTE (Synthetic Minority Over-sampling Technique) untuk mengatasi masalah distribusi kelas yang tidak merata. Selain itu, penggunaan pembelajaran tambahan (ensemble learning) telah menjadi strategi yang efektif dalam meningkatkan akurasi deteksi penipuan. Dengan menggabungkan beberapa model pembelajaran mesin, sistem dapat menjadi lebih tangguh terhadap perubahan pola penipuan.

Dalam keseluruhan analisis dan pembahasan, dapat disimpulkan bahwa teknologi IT memiliki potensi besar dalam deteksi penipuan kartu kredit, tetapi tantangan seperti ketersediaan data, distribusi kelas yang tidak merata, dan taktik penipuan yang terus berkembang tetap menjadi perhatian. Upaya terus menerus dalam pengembangan algoritme dan teknik deteksi diperlukan untuk menjaga langkah dengan penipuan kartu kredit yang semakin canggih.

V. Conclusion

Simpulan:

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.

Saran:

Dalam penerapan teknologi IT untuk deteksi penipuan kartu kredit perlu dicek Kembali apakah teknologi tersebut mampu mengatasi tantangan dan kendala yang ada seperti keterbatasan data, distribusi kelas yang tidak merata, dan mendeteksi 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 probabilistic 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>.
- [6] M.Zareapoor and P.vol 48, no. C, pp. 679-689, 2015.
- [7] A.Gupta, D. Kumar, and A. Address, " *Int. J. Comput. Appl.*, vol. 166, no. 5, pp. 33-37, 2017.
- [8] K.P. Murphy, *A probabilistic 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, Deutschland, 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).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

MATCHED SOURCES:

Polisi Tangkap Pelaku Penipuan dan Penggelapan ...

<https://analisadaily.com/berita/baca/2021/08/11/1020796/poli....> (<https://analisadaily.com/berita/baca/2021/08/11/1020796/polisi-tangkap-pelaku-penipuan-dan-penggelapan-melalui-aplikasi-online/>)

Paper Template

https://nvmts22.stanford.edu/files/NVMTS2022_Paper_Template..... (https://nvmts22.stanford.edu/files/NVMTS2022_Paper_Template.docx)

uscga.edu › wp-content › uploadsThe Journal of Cadet Research Academic Excellence at the US ...

https://uscga.edu/wp-content/uploads/2022/05/jcr_paper_templ.... (https://uscga.edu/wp-content/uploads/2022/05/jcr_paper_template.pdf/)

Paper Title (use style

<https://www.nist.gov/document/lorehlt16systemdescriptiontemp....> (<https://www.nist.gov/document/lorehlt16systemdescriptiontemplatedocx>)

Paragraph Spacing in the IEEEtran class using LaTeX

<https://tex.stackexchange.com/questions/467226/paragraph-spa....> (<https://tex.stackexchange.com/questions/467226/paragraph-spacing-in-the-ieee-tran-class-using-latex>)

docs.google.com › document › dPaper-Template-IEEE.doc - Google Docs

<https://docs.google.com/document/d/1uSI2mx9J-MC81QvIFjRZK-af....> (<https://docs.google.com/document/d/1uSI2mx9J-MC81QvIFjRZK-afyDaZkX7I/edit#!/>)

Paper Title (use style

<https://www.ieee.org/content/dam/ieee-org/ieee/web/org/confe....> (<https://www.ieee.org/content/dam/ieee-org/ieee/web/org/conferences/Conference-template-A4.doc>)

BAB IV METODE PENELITIAN

<http://repository.trisakti.ac.id/usaktiana/digital/000000000....>
(http://repository.trisakti.ac.id/usaktiana/digital/00000000000000093493/2017_TA_KD_03013129_Bab-4-Metode.pdf)

Iterative cleaning and learning of big highly-imbalanced fraud ...

<https://journalofbigdata.springeropen.com/articles/10.1186/s....> (<https://journalofbigdata.springeropen.com/articles/10.1186/s40537-023-00750-3>)

Teknik Pengambilan Sampel dalam Metode Penelitian ...

<https://adjar.grid.id/read/543626212/teknik-pengambilan-samp....> (<https://adjar.grid.id/read/543626212/teknik-pengambilan-sampel-dalam-metode-penelitian-kuantitatif?page=all>)

Penentuan Emosi pada Video dengan Convolutional Neural ...

<https://ejournal.uin-suka.ac.id/saintek/JISKA/article/downlo....> (<https://ejournal.uin-suka.ac.id/saintek/JISKA/article/download/51-04/1671>)

Report Generated on **October 23, 2023** by <https://www.check-plagiarism.com/> (<https://www.check-plagiarism.com/>)