**Tugas Kelompok ke- 4**

**Minggu 9**

**Team 3:**

1. Wulan Aprianingsih – 2502126554
2. Gilang Hansagita – 2502124403
3. Frans Sebsastian – 2502121162
4. Adam Candra Setianugraha – 2502121534

Tugas kelompok 4 ini merupakan kelanjutan dari tugas kelompok 2 dan 3 dengan menambahkan bagian dari artikel ilmiah yaitu bagian 4. **Review findings and discussions**, dan bagian 5, **conclusion**, seperti contoh artikel yang dapat diakses di [SLR](https://sci-hub.hkvisa.net/10.1016/j.cor.2020.104926). Beberapa hal yang harus anda kerjakan untuk menjawab tugas ini adalah:

1. Tuliskan analisis dan pembahasan hasil studi literatur dalam bentuk text berdasarkan rumusan masalah (research questions) yang sudah dituliskan di review methodology.

**Jawab:**

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.

2. Tuliskan bagian simpulan dan saran

**Jawab:**

* **Simpulan:**

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

1. Ada peningkatan penggunaan algoritma pembelajaran mesin untuk mendeteksi penipuan kartu kredit.
2. Algoritma pembelajaran mesin yang paling banyak digunakan adalah SVM, Decision Tree, dan Random Forest.
3. Teknik pengambilan sampel yang paling banyak digunakan adalah SMOTE.
4. 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.

3. Tuliskan daftar Pustaka minimal sebanyak 15 buah yang semuanya dicitasi dalam text artikel.

**Jawab**:

**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>.
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

4. Lakukan cek plagiarisme dari paper yang sudah anda selesaikan ini dengan menggunakan tools cek plagiarism tertentu dan hasilnya dibuat dalam bentuk file pdf yang disubmit bersamaan dengan jawaban tugas ini yang disatukan ke dalam zip file.

**Jawab:**

File sudah terlampir

5. Kriteria hasil cek plagiarism yang dapat dikumpulkan adalah kurang dari 15%

**Jawab**:

Berdasarkan hasil cek plagiarism maka dapat disimpulkan bahwa paper dari team 3