

Panduan Praktikum Deteksi Anomali

Durasi: 3 × 110 menit

Capaian Pembelajaran Mata Kuliah

Mahasiswa mampu menjelaskan konsep dan teknik deteksi anomali serta penggunaannya pada data anomali.

Tools

- Google Colab
- Jupyter Notebook
- PyCharm
- Spyder
- Python IDE yang lain

Materi Praktikum

- Pengertian Deteksi Anomali

Deteksi anomali adalah proses untuk mengidentifikasi pola data yang berbeda secara signifikan dari mayoritas data lainnya dalam dataset. Pola ini, yang disebut anomali atau outlier, dapat menunjukkan kejadian yang tidak biasa, seperti kesalahan, penipuan, atau aktivitas abnormal.

- Jenis-Jenis Anomali

1. ****Point Anomalies****

- Suatu data individu yang berbeda secara signifikan dari keseluruhan dataset.
- Contoh: Suhu mencapai 60°C di lokasi dengan suhu rata-rata 20°C.

2. ****Contextual Anomalies****

- Data yang hanya dianggap anomali dalam konteks tertentu.
- Contoh: Transaksi besar selama liburan mungkin normal, tetapi transaksi serupa di hari biasa dianggap anomali.

3. ****Collective Anomalies****

- Sekumpulan data yang bersama-sama membentuk pola anomali.
- Contoh: Serangkaian aktivitas yang menunjukkan serangan DDoS.

- Pentingnya Deteksi Anomali

1. ****Keamanan****

- Deteksi aktivitas yang mencurigakan seperti penipuan kartu kredit atau akses tidak sah.

2. ****Kesehatan****

- Identifikasi kondisi kesehatan abnormal berdasarkan data medis.

3. ****Pemeliharaan****

- Prediksi kegagalan mesin berdasarkan pola penggunaan yang tidak biasa.

4. ****Analisis Bisnis****

- Memahami pola penjualan yang tidak biasa.

- Metode Deteksi Anomali

1. ****Statistik****

- Menggunakan distribusi probabilitas untuk mengidentifikasi data yang jauh dari nilai rata-rata atau standar deviasi.

- Contoh: Z-Score, boxplot.

2. ****Berbasis Jarak (Distance-Based)****

- Mengukur jarak antara titik data untuk menentukan outlier.

- Contoh: K-Nearest Neighbors (KNN), DBSCAN.

3. ****Berbasis Densitas (Density-Based)****

- Mendeteksi anomali berdasarkan kepadatan data di sekitar titik tertentu.

- Contoh: Local Outlier Factor (LOF).

4. ****Berbasis Model (Model-Based)****

- Menggunakan model statistik atau pembelajaran mesin untuk mendeteksi

anomali.

- Contoh: Gaussian Mixture Models (GMM), Isolation Forest.

5. **Deep Learning**

- Memanfaatkan arsitektur jaringan saraf untuk mendeteksi anomali kompleks.
- Contoh: Autoencoder, GAN (*Generative Adversarial Networks*).

- Evaluasi Deteksi Anomali

1. **Precision dan Recall**

- Precision: Proporsi anomali yang terdeteksi dengan benar dari seluruh prediksi anomali.
- Recall: Proporsi anomali yang terdeteksi dengan benar dari seluruh anomali yang ada.

2. **Area Under Curve (AUC)**

- Mengukur kinerja model deteksi anomali dengan melihat trade-off antara precision dan recall.

3. **F1-Score**

- Menggabungkan precision dan recall menjadi satu metrik.

- Contoh Aplikasi Deteksi Anomali

1. **Deteksi Penipuan**

- Menggunakan data transaksi untuk mengidentifikasi aktivitas yang mencurigakan.
- Contoh: Aktivitas login tidak sah pada akun pengguna.

2. **Keamanan Siber**

- Mendeteksi pola trafik jaringan yang tidak biasa sebagai indikasi serangan.

3. **Pemeliharaan Prediktif**

- Mengidentifikasi pola operasi mesin yang menunjukkan potensi kegagalan.

4. **Analisis Medis**

- Mendeteksi pola abnormal dalam data pasien seperti denyut jantung atau tekanan darah.

Panduan Praktikum

Download lalu pelajari dan running code pada link berikut:

<https://github.com/aldinata/Modul-Praktikum-Data-Mining/blob/main/Materi/7%20-%20Deteksi%20Anomali.ipynb>