UNIVERSITAS
GADJAH MADA
Analisis dan Perbandingan Model Transformer Untuk Klasifikasi Tingkat Keparahan Common Vulnerabilities and Exposures Secara Otomatis
Aditya Darmasaputra, Ir. Yuris Mulya Saputra, S.T., M.Sc., Ph.D., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

ANALISIS DAN PERBANDINGAN MODEL TRANSFORMER UNTUK KLASIFIKASI TINGKAT KEPARAHAN *COMMON VULNERABILITIES AND EXPOSURES* SECARA OTOMATIS

Aditya Darmasaputra
21/480255/SV/19599

Pertumbuhan volume CVE yang dipublikasikan telah melampaui kapasitas analisis manual, sehingga menimbulkan jeda struktural antara publikasi CVE dan tersedianya label tingkat keparahan yang dapat diandalkan pada CVE List v5. Penelitian ini bertujuan membangun dan mengevaluasi sistem klasifikasi tingkat keparahan CVE ke dalam empat kelas (LOW, MEDIUM, HIGH, CRITICAL) menggunakan tiga model transformer *pre-trained*, yaitu DistilBERT, ModernBERT, dan SecureBERT, berdasarkan deskripsi tekstualnya. Ketidakseimbangan kelas ditangani melalui augmentasi EDA berbasis leksikon domain siber, dikombinasikan dengan *label smoothing* dan *cosine decay scheduler*. Penelitian ini juga mengembangkan sistem inferensi berbasis web menggunakan Streamlit dan FastAPI yang dikontainerisasi Docker, mencakup prediksi *batch*, komparasi tiga model, serta *benchmark latency*, *throughput*, dan utilisasi CPU. Hasil pengujian pada test set yang terisolasi dari augmentasi menunjukkan SecureBERT mencapai MCC tertinggi (0,5494), diikuti DistilBERT (0,5421) dan ModernBERT (0,4966), dengan keunggulan SecureBERT pada kelas HIGH dan CRITICAL berkat pemahaman terminologi domain siber. Augmentasi EDA efektif pada kelas berkosakata teknis banyak namun kurang berkontribusi pada kelas sebaliknya. Hasil *Benchmark* menunjukkan DistilBERT paling unggul dari sisi *latency* denga nilai rata-rata 448,29 ms dan *throughput* dengan total 302,27 kata/detik, sedangkan ModernBERT paling berat beban komputasinya dengan rata-rata 283,22%. Kesalahan klasifikasi ketiga model terkonsentrasi pada kelas bersebelahan, mengindikasikan pendekatan berbasis teks murni telah mendekati batas performa maksimalnya, sehingga diperlukan fitur CVSS terstruktur tambahan pada penelitian lanjutan.

Kata kunci: CVE, Transformer, *Easy Data Augmentation*, MCC, Streamlit, FastAPI, Docker

UNIVERSITAS
GADJAH MADA
Analisis dan Perbandingan Model Transformer Untuk Klasifikasi Tingkat Keparahan Common Vulnerabilities and Exposures Secara Otomatis
Aditya Darmasaputra, Ir. Yuris Mulya Saputra, S.T., M.Sc., Ph.D., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

ANALYSIS AND COMPARISON OF TRANSFORMER MODELS FOR AUTOMATIC CLASSIFICATION OF SEVERITY LEVEL OF COMMON VULNERABILITIES AND EXPOSURES

Aditya Darmasaputra
21/480255/SV/19599

The growing volume of published CVEs has exceeded manual analysis capacity, creating a structural delay between CVE publication and the availability of reliable severity labels within CVE List v5. This study aims to build and evaluate a CVE severity classification system across four classes (LOW, MEDIUM, HIGH, CRITICAL) using three pre-trained transformer models, namely DistilBERT, ModernBERT, and SecureBERT, based on their textual descriptions. Class imbalance was addressed through EDA augmentation based on a cybersecurity-domain lexicon, combined with label smoothing and a cosine decay scheduler. This study also developed a web-based inference system using Streamlit and FastAPI containerized with Docker, covering batch prediction, comparison of the three models, and benchmarking of latency, throughput, and CPU utilization. Evaluation on a test set isolated from augmentation shows that SecureBERT achieved the highest MCC (0.5494), followed by DistilBERT (0.5421) and ModernBERT (0.4966), with SecureBERT's advantage evident in the HIGH and CRITICAL classes due to its understanding of cybersecurity domain terminology. EDA augmentation proved effective for classes with rich technical vocabulary but contributed less to the opposite class. Benchmark results show that DistilBERT outperforms the others in terms of latency with an average of 448.29 ms and throughput with a total of 302.27 words/second,;meanwhile, ModernBERT imposes the heaviest computational load averaging 283.22%. Misclassifications across all three models were concentrated between adjacent classes, indicating that a purely text-based approach is approaching its maximum performance boundary, suggesting that future research incorporate additional structured CVSS features.

Keywords: CVE, Transformer, Easy Data Augmentation, MCC, Streamlit, FastAPI, Docker