Analisis Robustness Model Convolutional Neural Network terhadap Serangan Adversarial pada Skenario
Man-In-The-Middle untuk Klasifikasi Pneumonia Berbasis Chest X-Ray
Kharisma Sekarningtyas, 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 *ROBUSTNESS* MODEL *CONVOLUTIONAL NEURAL NETWORK* TERHADAP SERANGAN *ADVERSARIAL* PADA SKENARIO *MAN-IN-THE-MIDDLE* UNTUK KLASIFIKASI PNEUMONIA BERBASIS *CHEST X-RAY*

Kharisma Sekarningtyas
22/496804/SV/21012

Pneumonia merupakan penyebab utama kematian akibat infeksi global, sehingga diagnosis akurat menjadi sangat krusial. Meskipun *deep learning* telah menunjukkan potensi besar sebagai sistem pendukung keputusan klinis, model ini rentan terhadap serangan *adversarial*. Penelitian ini bertujuan untuk menganalisis *robustness* dari model EfficientNetB0, DenseNet121, dan ResNet50 terhadap serangan FGSM dan PGD pada sistem klasifikasi pneumonia berbasis *chest X-ray.* Evaluasi dilakukan melalui *offline evaluation* dan skenario *Man-in-the-Middle* (MITM) pada arsitektur *client-server* dengan menggunakan metrik *accuracy, precision, recall, F1-sore, latency,* dan *throughput.* Hasil menunjukkan akurasi pada data independen berkisar 85%–87%, lebih rendah dibandingkan akurasi validasi (>98%), yang menegaskan pentingnya proses pembagian *dataset* yang tepat untuk memperoleh estimasi generalisasi. DenseNet121 terbukti memiliki tingkat *robustness* terbaik, sementara EfficientNetB0 paling rentan terhadap perturbasi. Serangan PGD menurunkan akurasi hingga 0% pada *offline evaluation,* sedangkan pada skenario MITM akurasi masih bertahan pada kisaran 40%–65% akibat *transferability gap*. Skenario MITM juga meningkatkan *latency* lebih dari 10 kali lipat serta menurunkan *throughput* sebesar 90%–94% akibat proses pembentukan perturbasi. Temuan ini menunjukkan bahwa evaluasi akurasi saja belum memadai sehingga evaluasi *robustness* dan keamanan implementasi perlu dipertimbangkan sebelum sistem diterapkan pada lingkungan klinis.

Kata kunci : Pneumonia, *Chest X-ray, Adversarial Attack, Man-in-the-Middle, Robustness.*

UNIVERSITAS
GADJAH MADA
**Analisis Robustness Model Convolutional Neural Network terhadap Serangan Adversarial pada Skenario
Man-In-The-Middle untuk Klasifikasi Pneumonia Berbasis Chest X-Ray**
Kharisma Sekarningtyas, Ir. Yuris Mulya Saputra, S.T., M.Sc., Ph.D., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

ROBUSTNESS ANALYSIS OF CONVOLUTIONAL NEURAL NETWORKS AGAINST ADVERSARIAL ATTACKS IN MAN-IN-THE-MIDDLE SCENARIO FOR PNEUMONIA CLASSIFICATION USING CHEST X-RAY

Kharisma Sekarningtyas
22/496804/SV/21012

Pneumonia is the leading cause of death from infections globally, making accurate diagnosis crucial. Although deep learning has shown great potential as a clinical decision support system, these models are vulnerable to adversarial attacks. This study aims to analyze the robustness of the EfficientNetB0, DenseNet121, and ResNet50 models against FGSM and PGD attacks on a chest X-ray-based pneumonia classification system. The evaluation was conducted thru offline evaluation and Man-in-the-Middle (MITM) scenarios on a client-server architecture using the metrics of accuracy, precision, recall, F1-score, latency, and throughput. The results show that the accuracy on independent data ranges from 85% to 87%, lower than the validation accuracy (>98%), highlighting the importance of proper dataset partitioning to obtain generalization estimates. DenseNet121 proved to have the best robustness level, while EfficientNetB0 was the most vulnerable to perturbations. The PGD attack reduces accuracy to 0% in the offline evaluation, while in the MITM scenario, accuracy remains in the range of 40%–65% due to the transferability gap. The MITM scenario also increases latency by more than 10 times and decreases throughput by 90%–94% due to the perturbation formation process. These findings indicate that accuracy evaluation alone is insufficient, and therefore, robustness and implementation security evaluations need to be considered before the system is applied in a clinical environment.

Keyword: Pneumonia, Chest X-ray, Adversarial Attack, Man-in-the-Middle, Robustness.