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/

DAFTAR ISI

HALAMAN JUDUL ii
LEMBAR PENGESAHAN iii
PERNYATAAN BEBAS PLAGIASI iv
KATA PENGANTAR v
DAFTAR ISI vii
DAFTAR GAMBAR xi
DAFTAR TABEL xiv
DAFTAR SIMBOL xvi
INTISARI xvii
ABSTRACT xviii
BAB I PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Rumusan Masalah 4
1.3. Tujuan dan Manfaat Proyek Akhir 4
1.4. Batasan Penelitian 4
1.5. Sistematika Penulisan 5
BAB II KAJIAN PUSTAKA 7
2.1. Tinjauan Pustaka 7
2.2. Dasar Teori 21
2.2.1. Pneumonia 21
2.2.2. Medical Imaging 21
2.2.3. Chest X-ray 22
2.2.4. Analisis Data 23

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/

2.2.5. Deep Learning 24
2.2.6. *Convolutional Neural Network* (CNN) 25
2.2.7. EfficientNetB0 27
2.2.8. DenseNet121 27
2.2.9. ResNet50 28
2.2.10. Serangan *Adversarial* 29
2.2.11. Fast Gradient Sign Method 30
2.2.12. *Projected Gradient Descent* 31
2.2.13. Infrastruktur *Client-Server* 33
2.2.14. Man-in-the-Middle 34
2.2.15. SSL *Interception* 35
2.2.16. Evaluasi Kinerja Model 35
2.2.17. Quality of Service 37
2.3. Hipotesis 38
BAB III METODE PENELITIAN 39
3.1. Alat dan Bahan 39
3.1.1. *Dataset* 39
3.1.2. Perangkat Keras 39
3.1.3. Perangkat Lunak 39
3.2. Tahapan Proyek Akhir 40
3.2.1. Identifikasi Masalah 41
3.2.2. Studi Literatur 42
3.2.3. Perancangan Sistem 42
3.2.4. Pengembangan Sistem 44
3.2.5. Pengujian dan Analisis 44

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/

3.3. Perancangan Sistem 44
3.3.1. Arsitektur Sistem 45
3.3.2. Perancangan *Dataset* 48
3.3.3. Perancangan Model *Deep Learning* 53
3.3.4. Perancangan Metode Serangan *Adversarial* 57
3.3.5. Perancangan Tingkat Perturbasi *Adversarial* 60
3.3.6. Perancangan Alur Injeksi Adversarial melalui *Man-in-the-Middle* 61
3.4. Pengujian dan Analisis 65
3.4.1. Skenario Pengujian 65
3.4.2. Pengambilan Data Evaluasi Ketahanan Model Tanpa Serangan 66
3.4.3. Pengambilan Data Evaluasi Ketahanan Model pada Data *Adversarial* (*Offline Evaluation*) 67
3.4.4. Pengambilan Data Evaluasi Ketahanan Model pada Data *Adversarial* pada Skenario MITM 68
3.4.5. Pengambilan Data Performa Jaringan 68
BAB IV HASIL DAN PEMBAHASAN 72
4.1. Hasil Pelatihan Model 72
4.1.1. Hasil Pelatihan Model EfficientNetB0 72
4.1.2. Hasil Pelatihan Model DenseNet121 73
4.1.3. Hasil Pelatihan Model ResNet50 75
4.1.4. Ringkasan Hasil Pelatihan Model 76
4.2. Hasil Evaluasi Model Tanpa Serangan 77
4.2.1. Hasil Evaluasi Model Tanpa Serangan (*Offline Evaluation*) 78
4.2.2. Hasil Evaluasi Model Tanpa Serangan melalui Skenario *Client-Server* 79
4.2.3. Ringkasan Hasil Evaluasi Model Tanpa Serangan 79

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/

4.3. Hasil Evaluasi Model pada Data *Adversarial* (*Offline Evaluation*) 80
4.3.1. Evaluasi Model pada *Epsilon* 0,001 81
4.3.2. Evaluasi Model pada *Epsilon* 0,01 84
4.3.3. Evaluasi Model pada *Epsilon* 0,05 87
4.4. Hasil Evaluasi Model pada Data *Adversarial* melalui Skenario MITM..... 90
4.4.1. Evaluasi Model pada *Epsilon* 0,001 90
4.4.2. Evaluasi Model pada *Epsilon* 0,01 94
4.4.3. Evaluasi Model pada *Epsilon* 0,05 97
4.5. Ringkasan Hasil Evaluasi Model pada Data *Adversarial* 101
4.5.1. Perbandingan *Robustness* Antarmodel 101
4.5.2. Perbandingan *Offline Evaluation* dan Skenario MITM 103
4.6. Hasil Evaluasi Performa Jaringan 104
4.6.1. Analisis *Latency* 104
4.6.2. Analisis *Throughput* 106
BAB V PENUTUP 108
5.1 Kesimpulan 108
5.2 Saran 109
DAFTAR PUSTAKA 111
LAMPIRAN 121