

DAFTAR ISI

HALAMAN PENGESAHAN.....	ii
PERNYATAAN BEBAS PLAGIASI	iii
KATA PENGANTAR	iv
DAFTAR ISI.....	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL.....	x
INTISARI.....	xi
ABSTRACT.....	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Metodologi Penelitian	4
1.7 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA.....	7
BAB III DASAR TEORI	12
3.1 <i>Intrusion Detection System</i>	12
3.2 Protokol Jaringan.....	13
3.2.1 Serangan pada Protokol Jaringan.....	15
3.3 Taksonomi Algoritma Machine Learning	16
3.3.1 Artificial Neural Network.....	17
3.4 Pembuatan Data Sintetis.....	18
3.4.1 Generative Adversarial Network (GAN).....	19
3.4.2 Conditional Tabular Generative Adversarial Network (CT-GAN)	20
BAB IV RANCANGAN PENELITIAN	22
4.1 Analisis Sistem	22
4.2 Alat dan Bahan	23
4.3 Tahapan Penelitian	26
4.4 Arsitektur Sistem.....	28
4.4.1 Arsitektur Topologi Jaringan.....	29

4.4.2	Arsitektur IoT Web Server	30
4.4.3	Rancangan <i>Penetration Testing</i>	31
4.4.4	Penggunaan Dataset	32
4.4.5	Arsitektur Conditional Tabular GAN	33
4.4.6	Arsitektur Artificial Neural Network	35
4.5	Penilaian Sistem	37
BAB V IMPLEMENTASI		38
5.1	Implementasi Topologi Jaringan	38
5.2	Implementasi IoT Web Server	41
5.3	Implementasi Sintesis Data Menggunakan CT-GAN	44
5.4	Implementasi IDS Menggunakan Artificial Neural Network	51
5.5	Implementasi Visualisasi Dashboard	56
5.6	Implementasi Attacker Menggunakan Virtual Machine	58
5.7	Tahap Pengujian Sistem	59
5.7.1	Pengujian Kualitas Sintesis Data CT-GAN	60
5.7.1	Pengujian Kinerja Model ANN dalam Memprediksi Serangan	60
5.7.1	Pengujian Sistem IDS pada Attacking IoT Web Server	63
BAB VI HASIL DAN PEMBAHASAN		65
6.1	Hasil Pengujian Data Sintetis dari CT-GAN	65
6.2	Hasil Kinerja Model ANN dalam Memprediksi Serangan	67
6.	Hasil Pengujian Sistem IDS pada Attacking IoT Web Server	71
BAB VII KESIMPULAN DAN SARAN		76
7.1	Kesimpulan	76
7.2	Saran	77
DAFTAR PUSTAKA		78
LAMPIRAN		81