

DAFTAR ISI

HALAMAN PENGESAHAN.....	ii
PERNYATAAN BEBAS PLAGIASI	iii
PRAKATA.....	iv
DAFTAR ISI.....	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
INTISARI.....	xi
ABSTRACT.....	xii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	6
1.3 Batasan Masalah.....	6
1.4 Tujuan Penelitian.....	7
1.5 Manfaat Penelitian.....	7
1.6 Kontribusi Penelitian.....	7
BAB II TINJAUAN PUSTAKA.....	8
2.1 Penelitian model deteksi pada SCADA dengan Pembelajaran mesin (<i>Machine learning</i>).....	8
2.2 Penelitian penanganan ketidakseimbangan data pada model deteksi	13
2.3 Pengembangan model deteksi anomali dan klasifikasi multi kelas.....	17
BAB III LANDASAN TEORI.....	22
3.1 SCADA	22
3.2 Komponen SCADA.....	22
3.3 Arsitektur	24
3.4 Protokol Modbus	26
3.5 Attack Vektor	28
3.6 Teknik Deteksi	32
3.6.1 Signature	32
3.6.2 Anomali.....	32
Teknik berbasis Statistik	32
Teknik Berbasis Pengetahuan	33
Teknik Berbasis Pembelajaran Mesin.....	33
3.6.3 Spesifikasi	34
3.7 Model Deteksi dengan <i>Machine Learning</i>	34
3.8 <i>Deep Learning</i>	35
3.9 Autoencoder	35
3.10 Matriks evaluasi.....	37
3.11 Ketidakseimbangan Data	39
Adaptive Synthetic Sampling (ADASYN)	40
Edited Nearest Neighbors (ENN).....	41
3.12 Testbed.....	42
BAB IV METODE PENELITIAN	44
4.1 Analisa Sistem	44
4.2 Deskripsi Umum.....	44

4.3	Tahapan Penelitian	45
4.4	Rancangan skenario pada <i>virtual testbed</i>	46
4.4.1	Rancangan Simulasi Komunikasi Modbus	46
4.4.2	Rancangan Komunikasi Modbus di <i>Industrial Control System</i>	49
4.4.3	Rancangan Modbus Attack dengan <i>Man in The Middle Attack</i>	52
4.5	Rancangan skenario pada <i>Phisical Testbed</i>	53
4.6	Dataset	56
4.7	Pendekatan model <i>A Hybrid Autoencoder-based Tree detection</i>	59
4.7.1	Tahap Preprocessing	61
4.7.2	Tahap penyeimbangan data	62
4.7.3	Autoencoder	64
4.7.4	Tree detection	66
4.8	Evaluasi Model	67
BAB V	HASIL DAN PEMBAHASAN	69
5.1	Hasil skenario pada <i>virtual testbed</i>	69
5.1.1	Hasil Hacking Modbus protokol pada <i>Slave</i> dengan Metasploit	69
5.1.2	Hasil Hacking Modbus dengan Ettercap	72
5.1.3	Hasil Analisis paket pada Wireshark	72
5.2	Hasil skenario pada <i>Phisical Testbed</i>	75
5.2.1	Skenario Serangan <i>Denial of service</i>	81
5.2.2	Skenario Serangan Man-in-the-middle (MITM)	83
5.3	Performa model <i>balancing</i> data menggunakan <i>Deep-Hybrid</i>	85
5.3.1	Oversampling	86
5.3.2	Undersampling	87
5.3.3	Hybrid	89
5.3.4	<i>Ensemble Learning</i>	90
5.3.5	Model <i>Deep-Hybrid balancing</i>	91
5.4	Hasil analisis perbandingan model <i>Deep-Hybrid</i> dalam <i>balancing</i> data	92
5.5	Performa model deteksi dengan <i>A Hybrid Autoencoder-based Tree Detection</i>	95
5.6	Hasil analisis perbandingan model <i>A Hybrid Autoencoder-based Tree Detection</i>	97
BAB VI	KESIMPULAN DAN SARAN	99
6.1	Kesimpulan	99
6.2	Saran	99
DAFTAR PUSTAKA		100
DAFTAR LAMPIRAN		106