

DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	xi
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xv
ABSTRAK	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN.....	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	9
C. Batasan Masalah	9
D. Tujuan Penelitian	10
E. Manfaat Penelitian	10
BAB II TINJAUAN PUSTAKA.....	12
A. Landasan Teori.....	12
B. Penelitian Sebelumnya.....	30
BAB III METODE PENELITIAN.....	37
A. Metode Pengumpulan Data.....	37
B. Alat dan Bahan Penelitian.....	40
C. Konsep Penelitian	42
BAB IV HASIL DAN PEMBAHASAN	48
A. Hasil Analisis.....	48

B. Pembahasan.....	98
BAB V PENUTUP.....	112
A. Kesimpulan	112
B. Saran	114
DAFTAR PUSTAKA	
LAMPIRAN	

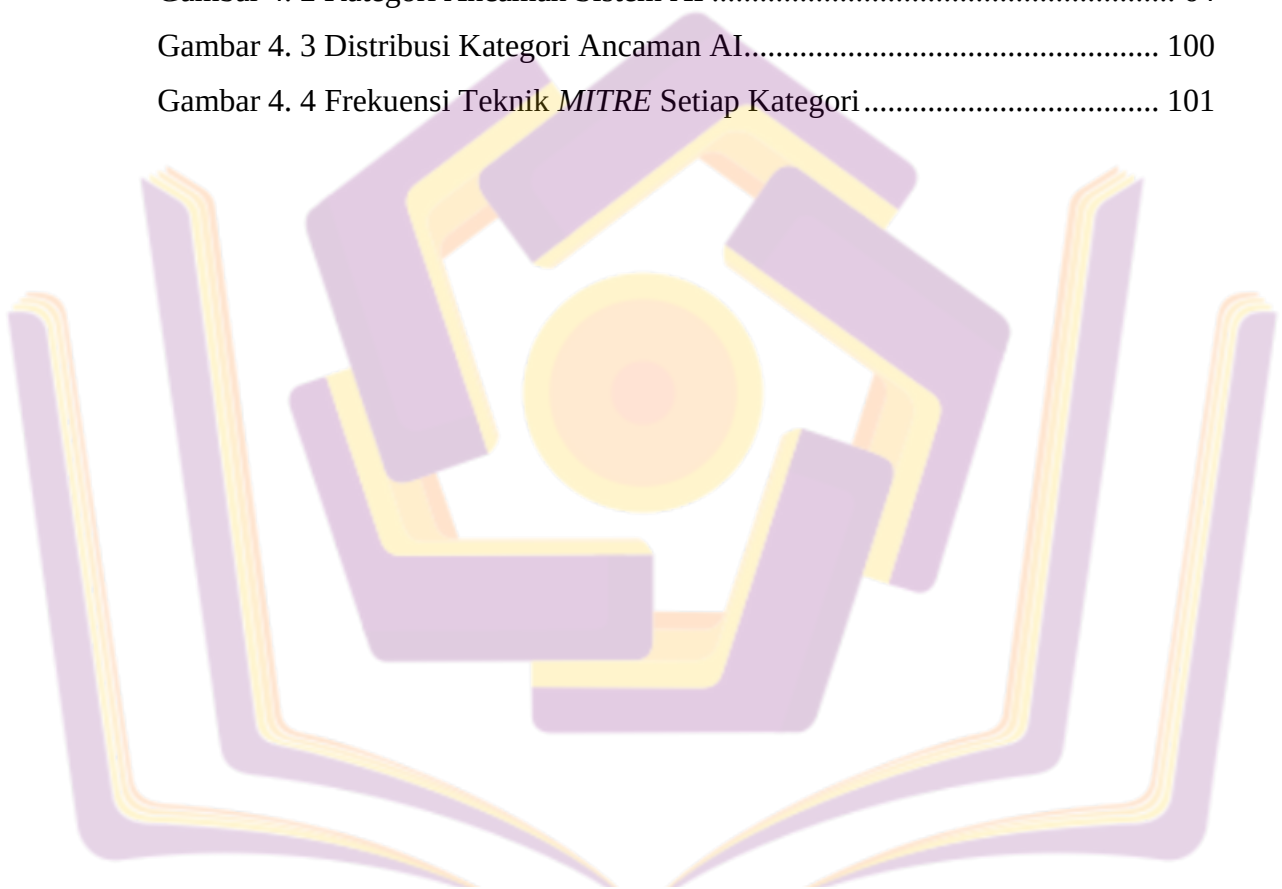


DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	34
Tabel 3. 1 Perangkat Keras	40
Tabel 3. 2 Perangkat lunak.....	41
Tabel 4. 1 Karakteristik Atribut Utama Dataset.....	49
Tabel 4. 2 Ringkasan Statistik Hasil Pembersihan dan Penyaringan Dataset.....	54
Tabel 4. 3 Contoh Data Hasil <i>Filtering</i>	57
Tabel 4. 4 Distribusi Frekuensi Teknik <i>MITRE Privacy Risks</i>	68
Tabel 4. 5 Distribusi Frekuensi Teknik <i>MITRE AI/ML Security</i>	68
Tabel 4. 6 Distribusi Frekuensi Teknik <i>MITRE AI Agents & LLM</i>	69
Tabel 4. 7 Kronologi Serangan <i>Data Exfiltration via Prompt Injection</i> T1606 ...	71
Tabel 4. 8 Kronologi Serangan <i>Intercept WebView Cookies</i> T1557	75
Tabel 4. 9 Kronologi Serangan <i>Prompt-In-Attribute Trick</i> T1059	78
Tabel 4. 10 Pelabelan <i>Attack Steps Data Exfiltration</i>	81
Tabel 4. 11 Pelabelan Serangan <i>Prompt-In-Attribute Trick</i>	86
Tabel 4. 12 Rekapitulasi Teknik <i>MITRE ATLAS</i>	89
Tabel 4. 13 Rekomendasi Mitigasi Teknik AML.T0051.....	91
Tabel 4. 14 Rekomendasi Mitigasi Teknik AML.T0056.....	93
Tabel 4. 15 Rekomendasi Mitigasi Teknik AML.T0057.....	96
Tabel 4. 16 Serangan Terpilih Berdasarkan Frekuensi Tertinggi	102
Tabel 4. 17 Hasil Rekonstruksi Kronologi Serangan.....	103
Tabel 4. 18 Hasil Pelabelan <i>Attack Steps</i> Menggunakan <i>MITRE ATLAS</i>	105
Tabel 4. 19 <i>Technique</i> dan <i>Mitigation</i>	108

DAFTAR GAMBAR

Gambar 1. 1 Kenaikan Penggunaan AI.....	3
Gambar 1. 2 Persentase Serangan AI.....	4
Gambar 2. 1 Rantai Tahapan Serangan.....	23
Gambar 2. 2 <i>Matriks MITRE ATLAS</i>	27
Gambar 3. 1 Alur Penelitian.....	43
Gambar 4. 1 Hasil <i>Executed</i> Penyaringan Data pada Terminal Python.....	55
Gambar 4. 2 Kategori Ancaman Sistem AI	64
Gambar 4. 3 Distribusi Kategori Ancaman AI.....	100
Gambar 4. 4 Frekuensi Teknik <i>MITRE</i> Setiap Kategori.....	101



DAFTAR LAMPIRAN

Lampiran 1 Sampel attack_dataset.csv

Lampiran 2 Dataset Hasil Filtering

Lampiran 3 *Source Code* Filtering

Lampiran 4 *Source Code* Pemecahan Kategori

Lampiran 5 *Source Code* Frekuensi Mitre Teknik Masing Masing Kategori

