

DAFTAR ISI

ABSTRAK	vii
ABSTRACT	viii
KATA PENGANTAR	ix
DAFTAR TABEL	vi
DAFTAR GAMBAR	vii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	2
1.6 Tahapan Penelitian	3
1.7 Sistematika Penulisan	4
BAB II TINJAUAN LITERATUR	5
2.1 Manajemen Jaringan Modern dan Masalahnya	5
2.2 Fenomena Alert Storm dalam Operasional Jaringan	5
2.3 Konsep Root Cause Analysis (RCA)	7
2.3.1 Definisi dan Tujuan RCA	7
2.3.2 Tantangan dalam Pelaksanaan RCA	7
2.3.3 Klasifikasi Pendekatan RCA	7
2.4 Keterbatasan Sistem Monitoring Tradisional	8
2.4.1 Ketergantungan pada Ambang Batas Statis	8
2.4.2 Fragmentasi Data dan Kurangnya Korelasi	8
2.4.3 Keterbatasan Interval Polling	8
2.5 Konsep Data Mining dan <i>Association Rule</i>	9
2.5.1 Knowledge Discovery in Databases	9
2.5.2 Definisi Data Mining pada Log Jaringan	9
2.5.3 Association Rule Mining	9
2.5.4 Algoritma FP-Growth	10
2.6 Teknologi Pendukung	10
2.6.1 MikroTik RouterOS dan Mekanisme Pengumpulan Data	10
2.6.2 Tantangan dan Klasifikasi Data Telemetry	11
2.6.3 Bahasa Pemrograman Python	11
2.7 Metode Analisis: Association Rule Mining	11
2.7.1 Definisi Transaksi dalam Log Jaringan	12
2.7.2 Ukuran Ketertarikan (Interest Measure)	12

2.7.3	Algoritma FP-Growth.....	13
2.8	Metrik Evaluasi Kerja.....	14
2.8.1	Confusion Matrix Deteksi Anomali.....	14
2.8.2	Akurasi Diagnosis (<i>Precision, Recall, F1-Score</i>).....	14
2.8.3	Rasio Reduksi Alarm (<i>Compression Rate</i>).....	15
2.9	Penelitian Terdahulu (State of the Art)	16
BAB III METODOLOGI PENELITIAN		19
3.1	Pengumpulan Data.....	20
3.1.1	Mekanisme Akuisisi Data.....	20
3.1.2	Perancangan Topologi Jaringan.....	21
3.1.3	Pembagian <i>Dataset</i>	22
3.2	<i>Pre-Processing</i>	22
3.2.1	Penggabungan Dataset.....	23
3.2.2	Pembersihan Data	23
3.2.3	Pemisahan kata	24
3.2.4	Filtrasi Fitur dan Penghapusan Kata Tidak Relevanele.....	24
3.2.5	Pembentukan Transaksi	24
3.3	Perancangan Arsitektur Sistem.....	25
3.3.1	Desain Topologi Jaringan	25
3.3.2	Pembangkitan Aturan dan Metrik Evaluasi	28
3.3.3	Arsitektur Perangkat Lunak.....	28
3.4	Strategi Implementasi Algoritma.....	29
3.4.1	Konfigurasi Parameter	31
3.4.2	Strategi Penyaringan Bertingkat.....	32
3.4.3	Pembentukan Basis Pengetahuan	33
3.4.4	Validasi dan Prioritas Masalah Menggunakan Lift Ratio.....	33
3.5	Perancangan Dasbor Pemantauan.....	34
3.5.1	Tabel Aliran Log.....	34
3.5.2	Tabel Akar Masalah	35
3.6	Perancangan Skenario Uji	35
3.6.1	Skenario Pengujian Gangguan Fisik	36
3.6.2	Skenario Pengujian Serangan Siber.....	36
3.6.3	Skenario Pengujian Kongesti Jaringan.....	37
3.7	Prosedur Evaluasi dan Metrik Kinerja.....	37
3.7.1	<i>Confusion Matrix</i>	38
3.7.2	Metrik Pengukuran Kinerja	38

BAB IV HASIL PENGUJIAN DAN PEMBAHASAN	40
4.1 Pengumpulan Data.....	40
4.1.1 Mekanisme Akuisisi Data.....	40
4.1.2 Topologi Jaringan	40
4.1.3 Rekapitulasi Dataset Hasil Akuisisi.....	41
4.2 Pra Pemrosesan.....	41
4.2.1 Penggabungan dan Pelabelan	41
4.2.2 Pembersihan Data	42
4.2.3 Pemisahan Kata	42
4.2.4 Filtrasi Fitur dan Penghapusan Kata Tidak Relevan	42
4.2.5 Pembentukan Transaksi	42
4.3 Implementasi Association Rule Mining	43
4.3.1 Penyeimbangan Data Matriks.....	43
4.3.2 Ekstraksi Pola Berulang	43
4.3.3 Penyetelan Parameter dan Pembentukan Aturan	43
4.4 Analisis Hasil Akar Masalah	44
4.4.1 Evaluasi Kinerja Parameter	44
4.4.2 Kondisi Jaringan Normal.....	44
4.4.3 Skenario Link Failure	45
4.4.4 Skenario Upstream Failure	45
4.4.5 Skenario DDOS Attack.....	46
4.4.6 Skenario Broadcast Storm	46
4.5 Implementasi dan Pengujian pada Dasbor	46
4.5.1 Integrasi Basis Aturan.....	47
4.5.2 Mekanisme Deteksi Real-Time	47
4.5.3 Visualisasi Diagnosa Antarmuka Pengguna	47
4.6 Evaluasi Performa Menggunakan Confusion Matrix	49
4.6.1 Metodologi Pengujian	49
4.6.2 Perhitungan Matriks Evaluasi.....	50
4.6.3 Evaluasi Rasio Reduksi	51
4.6.4 Analisis Performa Keseluruhan	51
BAB V PENUTUP	54
5.1 Kesimpulan.....	54
5.2 Saran	54
DAFTAR PUSTAKA	56

DAFTAR TABEL

Tabel 2.1 Definisi Anomali.....	6
Tabel 2.2 State of the art.....	17
Tabel 3.1 Skenario Fault Injection.....	21
Tabel 3.2 Contoh Data Mentah.....	23
Tabel 3.3 Transformasi Teks pada Tahap Pembersihan Data	23
Tabel 3.4 Pemisahan log menjadi kata - kata	244
Tabel 3.5 Kategori Kata Tidak Relevan.....	244
Tabel 3.6 Pembentukan kata menjadi Matriks <i>Boolean</i>	25
Tabel 3.7 Contoh Transaksi	33
Tabel 3.8 Contoh Hasil Basis Pengetahuan	333
Tabel 3.9 Klasifikasi Prioritas Diagnosis Berbasis Metrik Asosiasi	333
Tabel 3.10 Struktur Data Aliran Log Aktif.....	355
Tabel 3.11 Struktur Data Peringatan Akar Masalah	355
Tabel 3.12 Mekanisme Pengujian Gangguan Fisik	356
Tabel 3.11 Mekanisme Pengujian Serangan Siber	356
Tabel 3.11 Mekanisme Pengujian Kongesti Jaringan.....	357
Tabel 3.15 Skenario Pengujian	377
Tabel 3.16 Rancangan Pengujian Confusion Matrix Multi-Kelas.....	388
Tabel 4.1 Distribusi Data Hasil Penggabungan	41
Tabel 4.2 Kombinasi Parameter <i>Grid Search</i>	444
Tabel 4.3 Log Sistem Kondisi Stabil	444
Tabel 4.4 Log Sistem Kondisi <i>Link Failure</i>	455
Tabel 4.5 Log Sistem Kondisi <i>Upstream Failure</i>	455
Tabel 4.6 Log Sistem Kondisi <i>DDOS Attack</i>	466
Tabel 4.7 Log Sistem Kondisi <i>Broadcast Storm</i>	466
Tabel 4.8 Hasil Pengujian Confusion Matrix	499
Tabel 4.9 Hasil Metrik Pengukuran Kinerja.....	50
Tabel 4.10 Hasil Rasio Reduksi Alarm.....	51

DAFTAR GAMBAR

Gambar 3.1 Alur Metodologi Penelitian	20
Gambar 3.2 Diagram Pre-processing.....	23
Gambar 3.3 Topologi Jaringan Simulasi dan Manajemen Out-of-Band	26
Gambar 3.4 Topologi Jaringan Skala Besar	27
Gambar 3.5 Diagram Arsitektur Software.....	29
Gambar 3.6 Alur Algoritma FP-Growth.....	29
Gambar 3. 7 <i>Wireframe Dashboard</i>	34
Gambar 4.1 Tampilan Dashboard Kondisi Normal	47
Gambar 4.2 Tampilan Data Aliran Log Aktif dalam Dasbor.....	48
Gambar 4.3 Tampilan Data Akar Masalah dalam Dasbor	48