

ABSTRAK

Jaringan komputer modern sering kali menghasilkan ribuan baris log saat terjadi gangguan, memicu fenomena badai alarm (*alert storm*) yang menyebabkan kelelahan notifikasi (*alert fatigue*) pada administrator. Pendekatan pemantauan konvensional berbasis ambang batas statis terbukti kurang efektif karena tingginya tingkat alarm palsu dan kurangnya korelasi otomatis antar-kejadian. Penelitian ini bertujuan untuk membangun sebuah sistem log aggregator menggunakan teknik *Association Rule Mining* dengan algoritma FP-Growth sebagai mesin *Root Cause Analysis* (RCA) pada perangkat MikroTik guna memilah informasi redundan dan memampatkan volume log.

Pengujian dilakukan melalui simulasi jaringan menggunakan GNS3 yang menghasilkan 18.598 baris log mentah dari lima skenario: Normal, *Link Failure*, *Upstream Failure*, *DDoS Attack*, dan *Broadcast Storm*. Data kemudian diseimbangkan menggunakan teknik *random undersampling* menjadi 12.500 baris transaksi (2.500 baris per skenario) sebagai masukan algoritma. Berdasarkan pengujian *Grid Search*, sistem dievaluasi menggunakan konfigurasi parameter *Minimum Support* 0,1% dan *Minimum Confidence* 20% untuk mengekstraksi pola anomali di tengah aliran data log yang cepat.

Hasil pengujian menunjukkan bahwa model algoritma membangkitkan 58.373 aturan asosiasi dengan *macro recall* sebesar 44,56%. Tingkat *recall* yang menengah ini dipengaruhi oleh tingginya ambiguitas dan tumpang tindih fitur (*feature overlap*) pada teks log OSPF yang membuat aturan menjadi terlalu sensitif (*oversensitive*). Meskipun demikian, sistem ini terbukti sangat sukses memenuhi tujuan utamanya sebagai *log aggregator*, dibuktikan dengan capaian Rasio Reduksi Alarm (*Compression Rate*) sebesar 93,50%. Sistem secara tangguh mampu memampatkan 18.598 baris log mentah menjadi hanya 1.209 peringatan yang ringkas dan terarah. Hal ini membuktikan bahwa implementasi FP-Growth dan mekanisme agregasi berbasis waktu dapat diandalkan untuk meminimalkan beban kognitif (*cognitive overload*) administrator saat melakukan investigasi insiden di tengah kondisi badai alarm.

Kata Kunci: Analisis Akar Masalah, Penambangan Aturan Asosiasi, FP-Growth, Badai Alarm, MikroTik.

ABSTRACT

Modern computer networks often generate thousands of log lines during disruptions, triggering alert storms that cause alert fatigue among administrators. Conventional monitoring approaches based on static thresholds have proven ineffective due to high false alarm rates and a lack of automated event correlation. This study aims to build a log aggregator system using Association Rule Mining with the FP-Growth algorithm as a Root Cause Analysis (RCA) engine on MikroTik devices to filter redundant information and compress log volumes.

Testing was conducted through network simulation using GNS3, generating 18,598 raw log lines from five scenarios: Normal, Link Failure, Upstream Failure, DDoS Attack, and Broadcast Storm. The data was then balanced using a random undersampling technique into 12,500 transaction lines (2,500 lines per scenario) as the algorithm's input. Based on Grid Search testing, the system was evaluated using parameter configurations of 0.1% Minimum Support and 20% Minimum Confidence to extract anomaly patterns amidst rapid log data streams.

The test results showed that the algorithmic model generated 58,373 association rules with a macro recall of 44.56%. This moderate recall level was influenced by the high ambiguity and feature overlap in OSPF log texts, which made the rules oversensitive. Nevertheless, the system proved highly successful in fulfilling its main objective as a log aggregator, evidenced by achieving an Alarm Reduction Ratio (Compression Rate) of 93.50%. The system robustly compressed 18,598 raw log lines into only 1,209 concise and targeted alerts. This demonstrates that the implementation of FP-Growth and time-based aggregation mechanisms can be relied upon to minimize the cognitive overload of administrators when investigating incidents during an alert storm.

Keywords: *Root Cause Analysis, Association Rule Mining, FP-Growth, Alert Storm, MikroTik.*