ABSTRAK

Seiring perkembangan teknologi pada saat ini, kebutuhan layanan akses internet sebagai media komunikasi semakin meningkat. Peningkatan ini menyebabkan adanya anomali pada lalu lintas jaringan. Anomali tersebut, bisa terjadi karena adanya serangan *Distributed Denial of Service* (DDoS) yang sengaja dibuat maupun *Flashcrowd*, sebuah lonjakan besar pada lalu lintas jaringan internet karena jumlah *user* yang mengakses *server* naik secara signifikan pada suatu waktu. Dampak suatu anomali adalah membuat *user* tidak dapat mengakses layanan internet.

Jika dibiarkan begitu saja, anomali tersebut dapat merugikan banyak pihak, baik dari sisi *user* maupun penyedia layanan akses internet. Oleh sebab itu, diperlukan penelitian lebih lanjut untuk mendeteksi anomali yang terjadi. Anomali yang terjadi bisa dideteksi dengan menggunakan *Covariance Matrix*. Banyaknya data yang diuji oleh *Covariance Matrix* seringkali menjadi hambatan dalam waktu, untuk itu digunakan *Sliding window* untuk dapat mengatasi banyaknya jumlah data. Setelah didapatkannya matriks *Covariance,* maka langkah selanjutnya untuk deteksi anomali adalah dengan menggunakan metode *decision tree* untuk mengetahui jenis anomali yang terjadi.

Hasil pengujian yang diperoleh dari metode deteksi anomali yang digunakan adalah didapatkannya keluaran jenis anomali yang terjadi, dan dari output tersebut dapat dihitung nilai keakuratan dalam mendeteksi *(Detection rate)* dan nilai kesalahan mendeteksi *(False positive rate)*. Suatu metode deteksi anomali yang bagus adalah dapat mendeteksi anomali dengan parameter nilai *Detection rate* yang tinggi dengan *False positive rate* yang rendah.

Kata kunci : deteksi anomali, *Covariance Matrix*, *Sliding Window*, *Decision tree*, *Detection rate*, *False positive rate*