BAB 5
PENUTUP

5.1 Kesimpulan

Setelah dilakukan penelitian terhadap prediksi serangan dengan menggunakan HMM dengan data yang digunakan ialah *access log* dan *error log* dari *website* SIAKAD UPNVJ, sehingga dapat disimpulkan sebagai berikut.

1. Hasil evaluasi yang didapat dengan melakukan percobaan sebanyak tiga skenario ialah.
   - Skenario 1 dengan pembagian data *training* 70% dan *testing* 30% menghasilkan akurasi 75.33%, presisi 90.02%, dan *recall* 14.4%.
   - Skenario 2 dengan pembagian data *training* 80% dan *testing* 20% menghasilkan akurasi 77.83%, presisi 88.64%, dan *recall* 13.13%.
   - Skenario 3 dengan pembagian data *training* 90% dan *testing* 10% menghasilkan akurasi 78.28%, presisi 89.7%, dan *recall* 13.5%
2. Hasil evalusi dari 3 Skenario menunjukan bahwa model dapat memprediksi sebuah serangan (kelas attack) di atas 85%, keakuratan dalam memprediksi serangan dan tidak serangan ialah 70%, namun untuk ketepatan model dalam memprediksi kelas sebenarnya pada data. Dari banyaknya kelas serangan pada data sebenarnya, hanya dibawah 15% model dapat memprediksi benar. Sehingga model kurang baik dalam memprediksi serangan dikarenakan adanya *imbalance* pada data.
3. Pada SIM terlihat berbagai macam akses yang mencurigakan seperti akses yang berasal dari Singapura, Amerika Serikat bagian Los Angles, dan Cina. Lalu terdapat perangkat mencurigakan seperti perangkat *other* yang tidak terdeteksi web server Apache, dan perangkat *Spyder*.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, diperlukannya suatu pengujian dan pengembangan penelitian lebih lanjut mengenai data dan hasil prediksi dengan menggunakan HMM agar menjadi lebih baik dan sistem lebih tepat dalam memprediksi. Saran untuk penelitian ini ialah sebagai berikut.

1. Penambahan sumber data *log* seperti *log firewall*, *log* IDS, *log database*, dan data *log* lainnya agar data lebih bervariatif dalam segala macam *behaviour client* dalam mengakses *website* sehingga pembangunan model probabilitas bisa lebih baik.
2. Penambahan *observation state* yaitu pada *method* seperti HEAD, PUT, TRACE, OPTIONS, dan DELETE agar model dapat membaca data baru tersebut.
3. Melakukan penambahan klasifikasi lebih detail yaitu seperti serangan apa atau jenis serangan apa yang terjadi dan juga dampak apa yang diberikan dalam serangan tersebut.
4. Dengan data yang *imbalance* sehingga diperlukan penambahan metode *oversampling* ataupun *undersampling* agar jumlah kelas *attack* dan *non-attack* seimbang.
5. Penambahan sistem yang bisa mendeteksi suatu akses yang dilakukan dengan menggunakan VPN (*Virtual Private Network*) atau dengan *Proxy Server* agar lokasi asal akses dapat diketahui lebih akurat.