Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

Team project ©2017
Dony Pratidana S. Hum | Bima Agus Setyawan S. IIP

BAB V

SIMPULAN DAN SARAN

5.1. Simpulan

Berdasarkan dari hasil penelitian yang dilakukan, mengimplementasikan *Count-Min Sketch* pada *Anomaly Detection System* dapat mengurangi akurasi pendeteksian, namun akurasi tidak berkurang secara signifikan jika menggunakan ukuran *hashtable* yang besar (dengan Epsilon lebih rendah dari 0.0001 dan Delta yang lebih rendah dari 0.0001).

Penggunaan fungsi *hash* yang berbeda pada *Count-Min Sketch* juga dapat mempengaruhi kecepatan prediksi. Hasil penelitian menunjukkan penggunaan fungsi *Mumurhash* menghasilkan kecepatan prediksi yang 5.48 lebih cepat dibandingkan dengan *Universal Hash* pada 256 *distinct flow* dan 21.94 kali lebih cepat pada 8192 *distinct flow*. Sehingga akan lebih baik jika menggunakan fungsi *Mumurhash3* untuk mendapatkan kecepatan prediksi yang lebih baik.

Hasil penelitian juga menunjukkan bahwa *Count-min Sketch* dapat menghasilkan prediksi pada lalu lintas anomali 20.68 kali lebih cepat dibandingkan dengan *Linked-List* pada ukuran window sebesar 30000. Sehingga *Count-Min Sketch* lebih baik diimplementasikan pada *Anomaly Detection System* berbasis *Naïve Bayes* untuk mendeteksi serangan *SYN Flood* pada lalu lintas jaringan yang mempunyai aktifitas lalu lintas yang tinggi dan mempunyai banyak *distinct flow* (Diatas 2000 *distinct flow* per detik). Karena *Count-Min Sketch* mempunyai keunggulan dalam kecepatan prediksi saat menggunakan *packet count window* yang besar dan mempunyai *distinct flow* yang banyak.

Namun, jika *Anomaly Detection System* berbasis *Naïve Bayes* digunakan untuk mendeteksi serangan *SYN Flood* pada lalu lintas jaringan yang mempunyai aktifitas lalu lintas yang rendah dan mempunyai jumlah *distinct flow* yang rendah (Dibawah 2000 *distinct flow* per detik), lebih baik mengimplementasikan struktur data *Linked-List*. Karena berdasarkan dari hasil penelitian *Linked-List* menghasilkan kecepatan prediksi 34.57 kali lebih cepat dibandingkan dengan *Count-Min Sketch* saat menggunakan *packet count window* berukuran 100 dan jika lalu lintas jaringan yang diprediksi mempunyai jumlah *distinct flow* yang rendah.

5.2. Saran

Berdasarkan dari hasil penelitian yang telah dilakukan, penulis dapat mengusulkan beberapa saran berikut :

1. *Count-Min Sketch* diimplementasikan pada *Anomaly Detection System* yang menggunakan teknik *machine learning* yang lainnya.
2. Penelitian dapat dilanjutkan dengan membandingkan performa *Count-Min Sketch* menggunakan fungsi *hash* yang lebih cepat dari *MurmurHash*.
3. Penelitian dapat dilanjutkan untuk menentukan nilai ukuran *hashtable* yang optimal sesuai dengan ukuran *packet count window*.

UNIVERSITAS MULTIMEDIA NUSANTARA