IMPLEMENTASI *COUNT-MIN SKETCH* PADA *ANOMALY DETECTION SYSTEM* BERBASIS *NAÏVE BAYES*

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Komputer

Nelson Wijaya
13110210003

PROGRAM STUDI SISTEM KOMPUTER
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2018

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI *COUNT-MIN SKETCH* PADA *ANOMALY DETECTION SYSTEM* BERBASIS *NAÏVE BAYES*

Oleh

Nama : Nelson Wijaya

NIM : 13110210003

Program Studi : Sistem Komputer

Fakultas : Teknik dan Informatika

Tangerang, 12 Februari 2018

Ketua Sidang

Fransiscus Ati Halim, S.Kom, M.M.

Dosen Penguji

Samuel Hutagalung, M.T.I

Dosen Pembimbing I

Hargyo Tri Nugroho, S.Kom., M.Sc.

Disahkan oleh,

Ketua Program Studi Sistem Komputer

Hargyo Tri Nugroho, S.Kom., M.Sc.

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya,

Nama	: Nelson Wijaya
NIM	: 13110210003
Program Studi	: Sistem Komputer
Fakultas	: Teknik dan Informatika

Menyatakan bahwa skripsi yang berjudul "IMPLEMENTASI *COUNT-MIN SKETCH* PADA *ANOMALY DETECTION SYSTEM* BERBASIS *NAÏVE BAYES*" ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan / penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 12 Februari 2018

Nelson Wijaya

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa yang selalu menyertai selama masa pengerjaan skripsi dan laporan skripsi berjudul "IMPLEMENTASI *COUNT-MIN SKETCH* PADA *ANOMALY DETECTION SYSTEM* BERBASIS *NAÏVE BAYES*" sehingga dapat diselesaikan dengan baik dan benar. Skripsi ini diajukan kepada Program Studi Sistem Komputer, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara.

Penyelesaian skripsi ini juga dibantu dan didukung oleh berbagai pihak, seperti teman-teman, dosen-dosen pembimbing, dan keluarga. Oleh karena itu, ucapan terima kasih yang sebesar-besarnya diucapkan kepada:

1. Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara,
2. Hira Meidia, Ph. D., selaku Wakil Rektor Bidang Akademik dan Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara,
3. Ir. Andrey Andoko, M.Sc., selaku Wakil Rektor Bidang Ad*min*istrasi Umum dan Keuangan,
4. Ika Yanuarti, S.E., MSF., selaku Wakil Rektor Bidang Kemahasiswaan,
5. Prof. Dr. Muliawati G. Siswanto, M.Eng.Sc., selaku Wakil Rektor Bidang Hubungan dan Kerjasama,
6. Hargyo Tri Nugroho, S.Kom., M.Sc., Ketua Program Studi Sistem Komputer Universitas Multimedia Nusantara dan dosen pembimbing pengerjaan skripsi yang selalu memberikan saran dan motivasi selama proses pengerjaan skripsi ,
7. Kedua orang tua serta kakak yang selalu mendukung selama proses pengerjaan skripsi,
8. Seluruh rekan mahasiswa program studi Sistem Komputer yang telah mendukung dan membantu,

Semoga skripsi ini dapat bermanfaat bagi pembaca, baik sebagai informasi maupun sumber inspirasi, terutama untuk mahasiswa Universitas Multimedia Nusantara dalam mengembangkan teknologi informasi dan komunikasi.

Tangerang, 12 Februari 2018

Nelson Wijaya

IMPLEMENTASI *COUNT-MIN SKETCH* PADA ANOMALY DETECTION SYSTEM BERBASIS NAÏVE BAYES

ABSTRAK

Anomaly Detection System merupakan sebuah sistem yang mendeteksi adanya aktifitas anomali pada jaringan komputer yang berpotensi merupakan sebuah serangan cyber seperti *Distributed Denial Of Service*. *Distributed Denial of Service* merupakan sebuah teknik penyerangan dimana penyerang mengirim paket lalu lintas jaringan pada sebuah *host* dari berbagai sumber untuk menghentikan layanannya pada jaringan. Salah satu teknik pendeteksian *Anomaly Detection System* merupakan *Machine Learning* berbasis *Naive Bayes Algorithm* yang mengklasifikasikan sebuah lalu lintas berdasarkan dari data lalu lintas anomali dan lalu lintas normal yang dipelajari oleh program. Penelitian ini mengimplementasikan sebuah struktur data *Count-Min Sketch* pada sebuah *Anomaly Detection System* berbasis teknik *machine learning Naïve Bayes*. Sistem yang dikembangkan dapat mendeteksi terjadinya sebuah penyerangan DDoS *SYN Flood* dengan menganaliskan setiap *distinct flow*. Hasil pengujian menunjukkan bahwa mengimplementasikan *Count-Min Sketch* pada *Anomaly Detection System* menghasilkan performa dalam segi kecepatan deteksi yang lebih baik dibandingkan dengan struktur data *Linked-List* jika menggunakan ukuran *packet count window* yang lebih besar dan lalu lintas jaringan yang diprediksi mempunyai *distinct flow* yang banyak. Penggunaan *Count-Min Sketch* mempunyai sedikit pengaruh terhadap prediksi akurasi dibandingkan dengan *Linked-List*, jumlah kesalahan prediksi yang diberikan bergantung pada ukuran *hashtable* yang digunakan oleh *Count-Min Sketch.*

Kata Kunci : *Count-Min Sketch* , *Linked-List*, Naïve Bayes, *Anomaly Detection System, Distinct flow*

IMPLEMENTATION OF COUNT-*MIN SKETCH* ON NAÏVE BAYES ANOMALY DETECTION SYSTEM

ABSTRACT

Anomaly Detection System is a system that detects a potentially malicious activity on a computer network. One of which is a Distributed Denial of Service Attack or DDoS. DDoS is a techinique which involves an attacker to send a multiple network packet to a victim host to disable its service in a network. A Machine Learning technique with a Naïve Bayes Algorithm is one of an Anomaly Detection techniques, this techinque classifies a network traffic based on a data learned by normal traffic and anomalious traffic. This research implements Count-Min Sketch data structure on a Naïve Bayes Anomaly Detection System. The system is designed to be able to detect a DDoS SYN Flood by analyzing every distinct flows in a network traffic. The results shows that implementing Count-Min Sketch on a Naïve Bayes Anomaly Detection System improves its detection speed compared to using a linear data structure linked-list. But the improvement of the detection speed can be seen when using a larger packet count window size and the network traffic analyzed contains a lot of distinct flows. Implementing Count-Min Sketch also affects the accuracy of the prediction by a small error compared to linked-list, the number of prediction errors depends on the size of the hashtable used on the Count-Min Sketch.

Keyword : Count-Min Sketch, Linked-List, Naïve Bayes, Anomaly Detection System, Distinct Flow

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL