



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk mengubah, 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.

**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

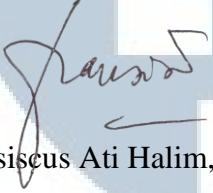
Program Studi : Sistem Komputer

Fakultas : Teknik dan Informatika

Tangerang, 12 Februari 2018

Ketua Sidang

Dosen Pengaji


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

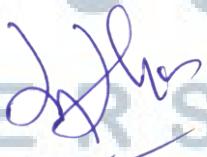

Samuel Hutagalung, M.T.I

Dosen Pembimbing I


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

Disahkan oleh,

Ketua Program Studi Sistem Komputer


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

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

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

**UNIVERSITAS
MULTIMEDIA
NUSANTARA**

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa yang selalu menyertai selama masa penggerjaan 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 Administrasi 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 penggerjaan skripsi yang selalu memberikan saran dan motivasi selama proses penggerjaan skripsi ,
7. Kedua orang tua serta kakak yang selalu mendukung selama proses penggerjaan 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 pendekripsi *Anomaly Detection System* merupakan *Machine Learning* berbasis *Naïve 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 technique 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 technique classifies a network traffic based on a data learned by normal traffic and anomalous 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

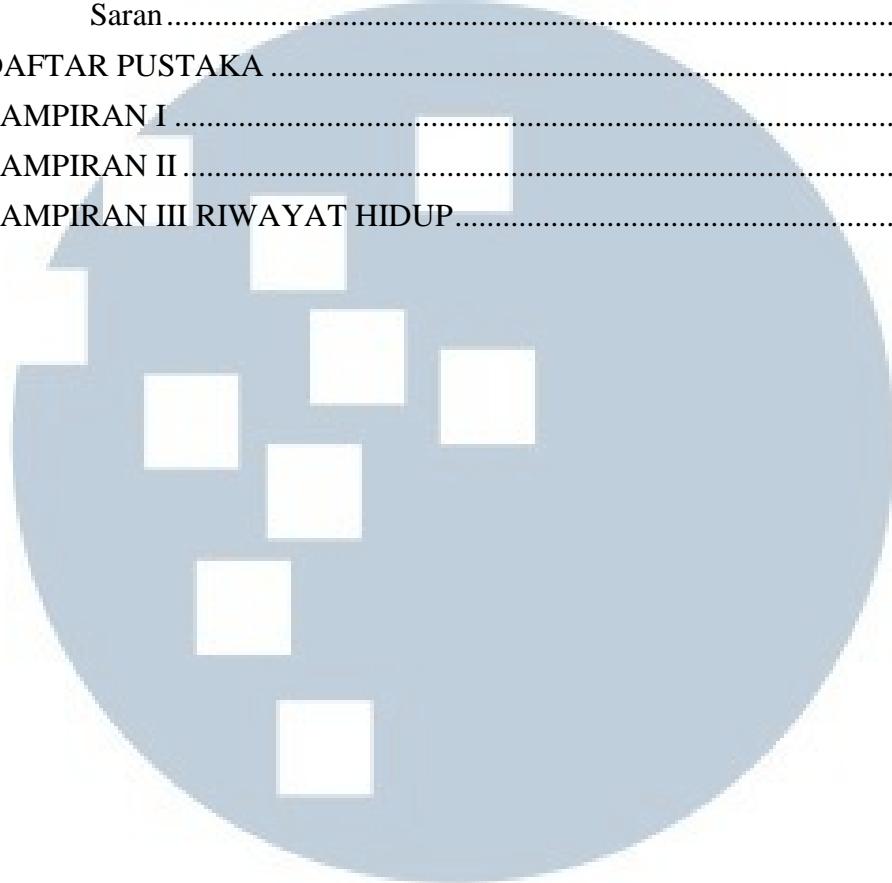


DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI	I
PERNYATAAN TIDAK MELAKUKAN PLAGIAT	II
KATA PENGANTAR	III
ABSTRAK	V
ABSTRACT	VI
DAFTAR ISI.....	VII
DAFTAR GAMBAR	X
DAFTAR TABEL.....	XI
BAB I PENDAHULUAN.....	1
Latar Belakang	1
1.1. Rumusan Masalah	3
1.2. Batasan Masalah.....	3
1.3. Tujuan Penelitian.....	3
1.4. Manfaat Penelitian.....	3
1.5.	
BAB II Tinjauan Pustaka	5
2.1. <i>Denial-Of-Service (DOS)</i>	5
2.2. <i>SYN Flood</i>	6
2.3. <i>Linked-List</i>	8
2.4. Pemeriksaan Elemen Baru	9
2.4.1. <i>Count-Min Sketch</i>	9
2.4.2. Prosedur Update	10
2.4.3. Point Query	11
2.5.	
2.6. Periksa Elemen Baru	11
2.7. 2.7.1. <i>Universal Hash</i>	12
2.7.2. <i>MurmurHash</i>	13
2.7.3. <i>Naïve Bayes Classifier</i>	15
Teori Dasar.....	15
Fase Training.....	16
Fase Prediksi	17
BAB III METODE PENELITIAN.....	18

Diagram Blok Arsitektur Sistem	18
Diagram Alur Paket Sniffer	19
Diagram Alur <i>Count-Min Sketch</i>	20
3.1. Diagram Alur Naïve Bayes Classifier.....	25
3.1.1. Uji Banding dan Performa	28
3.1.2. Instrumen Penelitian.....	32
3.1.3. BAB IV IMPLEMENTASI DAN PENGUJIAN.....	33
3.1.4. Implementasi <i>Count-Min Sketch</i> pada Program.....	33
3.2. Constructor.....	33
4.1. MurmurHash.....	34
4.1.1. Universal Hash.....	36
4.1.2. Update	37
4.1.4. Query.....	38
4.1.5. New Key Check	39
4.1.6. Pengujian <i>Count-Min Sketch</i>	40
4.2. Program Naïve Bayes Classifier.....	40
4.2.1. Menambahkan Data ke Dataset.....	41
4.2.2. Training.....	41
4.2.4. Kalkulasi Distribusi Normal	42
4.3. Prediksi.....	42
4.3.1. Program Utama.....	43
4.4. Training	43
4.4.1. Pengimplementasian <i>Count-Min Sketch</i>	44
4.4.2. Uji Banding dan Performa.....	46
4.4.3. Uji Kecepatan Menggunakan Banyak <i>Distinct flow</i>	46
Pengujian Implementasi pada Naïve Bayes	51
Pengujian Variasi Ukuran <i>Hashtable</i>	57
BAB V SIMPULAN DAN SARAN	61

Simpulan.....	61
Saran.....	62
DAFTAR PUSTAKA	63
LAMPIRAN I	66
5.1. LAMPIRAN II	68
5.2. LAMPIRAN III RIWAYAT HIDUP.....	71



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR GAMBAR

Gambar 2.1 Visualisasi SYN Flood Attack [23].....	7
Gambar 2.2 Struktur Serangan SYN Flood.....	8
Gambar 2.3 Visualisasi Struktur Data Linked-List [11]	8
Gambar 2.4 Visualisasi Prosedur Update [13].....	10
Gambar 3.1 Diagram Blok Sistem Anomaly Detection.....	18
Gambar 3.2 Diagram Alur paket sniffer, ekstraksi fitur paket dan buffer fitur paket	19
Gambar 3.3 Diagram alur inisiasi Count-Min Sketch.....	20
Gambar 3.4 Diagram Alur untuk Prosedur Update.....	21
Gambar 3.5 Diagram Alur untuk Prosedur Point Query	23
Gambar 3.6 Diagram alur periksa ketersediaan counter	24
Gambar 3.7 Diagram Alur Training Naive Bayes	26
Gambar 3.8 Diagram Alur Prediksi Naive Bayes Classifier.....	27
Gambar 3.9 Lalu lintas Anomali yang dihasilkan.....	30
Gambar 3.10 Lalu lintas Normal yang digunakan	31
Gambar 4.1 Kode inisiasi Count-Min-Sketch.....	33
Gambar 4.2 Hasil inisiasi Count-Min-Sketch	34
Gambar 4.3 Bagian 1 kode dari library murmurhash.....	35
Gambar 4.4 Bagian 2 kode dari library murmurhash.....	36
Gambar 4.5 Kode Universal Hash Function	37
Gambar 4.6 Kode Perbaruan Count pada Count-Min-Sketch menggunakan MurmurHash	37
Gambar 4.7 Kode Pengambilan Count pada Count-Min-Sketch	38
Gambar 4.8 Kode Pemeriksaan Key Baru pada Count-Min-Sketch.....	39
Gambar 4.9 Hasil pengujian Count-Min Sketch	40
Gambar 4.10 Visualisasi Linked-List	41
‘Gambar 4.11 Visualisasi akumulasi data paket pada Linked-List.....	44
Gambar 4.12 Visualisasi Implementasi Count-Min Sketch.....	45
Gambar 4.13 Contoh Hasil.....	46
Gambar 4.14 Grafik Waktu Pemrosesan Distinct flow dalam Mikrosekon.....	47
Gambar 4.15 Jumlah alokasi memori pada struktur data	49
Gambar 4.16 Hasil dari Valgrind memory checker tool	49
Gambar 4.17 Jumlah Pengalokasian Memori dengan ukuran Hashtable yang berbeda	50
Gambar 4.18 Hasil prediksi lalu lintas normal	52
Gambar 4.19 Hasil prediksi lalu lintas anomali	53
Gambar 4.20 Waktu Prediksi Lalu Lintas Anomali	54
Gambar 4.21 Waktu Prediksi Lalu Lintas Normal.....	56
Gambar 4.22 Distribusi Normal Pada Hashtable Berukuran Besar	58
Gambar 4.23 Distribusi Normal Pada Hashtable Berukuran Kecil	59

DAFTAR TABEL

Tabel 2.1 Tes banding performa dengan berbagai algoritma hash [15].....	14
Tabel 4.1 Kecepatan proses pada jumlah distinct flow yang berbeda	47
Tabel 4.2 Ukuran Hashtable berdasarkan dari Epsilon dan Delta	50
Tabel 4.3 Hasil Uji Akurasi Prediksi Naive Bayes	51
Tabel 4.4 Kecepatan prediksi lalu lintas anomali	54
Tabel 4.5 Kecepatan prediksi lalu lintas normal	55
Tabel 4.6 Hasil prediksi lalu lintas normal	57
Tabel 4.7 Hasil prediksi lalu anomali	58

