OPTIMASI *NAIVE BAYES* UNTUK KLASIFIKASI DENGAN *PARTICLE SWARM OPTIMIZATION*

Diajukan Sebagai Syarat Untuk Menyelesaikan

Pendidikan Program Strata-1 Pada

Jurusan Teknik Informatika

Oleh :

Cokro Nurwinto

NIM : 09021381520079

JURUSAN TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2020

LEMBAR PENGESAHAN TUGAS AKHIR

OPTIMASI *NAIVE BAYES* UNTUK KLASIFIKASI SERANGAN DDOS DENGAN *PARTICLE SWARM OPTIMIZATION*

Oleh :

Cokro Nurwinto
NIM : 09021381520079

Palembang, Juli 2020

Pembimbing I	Pembimbing II
Dian Palupi Rini, M.Kom., Ph.D.	Deris Stiawan, M.T., Ph.D.
NIP. 197802232006042002	NIP. 197806172006041002

Mengetahui,
Ketua Jurusan Teknik Informatika,

Rifkie Primartha, M.T
NIP. 197706012009121004

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari tanggal 23 Juli 2020 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Cokro Nurwinto

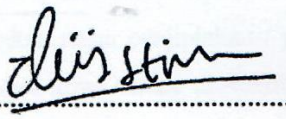
NIM : 09021381520079

Judul : Optimasi Naive Bayes untuk Klasifikasi Serangan DDoS dengan Particle Swarm Optimization

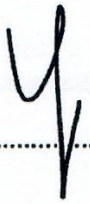
1. a.n Pembimbing I,

   Dian Palupi Rini, M.Kom., Ph.D.
   NIP. 197802232006042002 ..... 

2. Pembimbing II

   Deris Stiawan, M.T., Ph.D.
   NIP. 197806172006041002 ..... 

3. Penguji I

   Yunita, M.Cs.
   NIP. 198306062015042002 ..... 

4. Penguji II

   Danny Matthew Saputra, M.Sc.
   NIP. 198505102015041002 ..... 

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha, M.T
NIP. 197706012009121004

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Cokro Nurwinto
NIM : 09021381520079
Program Studi : Teknik Informatika
Judul Skripsi : Optimasi *Naïve Bayes* untuk Klasifikasi Serangan DDoS dengan *Particle Swarm Optimization*

Hasil pengecekan software *iTheticate / Turnitin* : 7%

Menyatakan bahwa laporan proyek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan proyek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan dari pihak manapun.

Palembang, Juli 2020

Cokro Nurwinto
09021381520079

MOTTO DAN PERSEMBAHAN

MOTTO :

"Don't think too hard, it makes you stupid."

Kupersembahkan karya tulis ini kepada :

- *Kedua Orang tua, adik, dan nyai tercinta*
- *Teman-teman Informatika 2015*
- *Fakultas Ilmu Komputer*
- *Universitas Sriwijaya*

NAÏVE BAYES OPTIMIZATION FOR DDOS CLASSIFICATION WITH PARTICLE SWARM OPTIMIZATION

By :
Cokro Nurwinto
09021381520079

ABSTRACT

DDoS is one of dangerous internet / cyber attacks. One of solution for overcoming the problem with identifying a traffic network wheter if it contains DDoS attack or not. Identification requires a lot of data for recognizing the pattern of DDoS attack so that it can be prevented as soon as possible. But, the traffic network it self has contain a lot of data per seconds. Therefore, a classification algorithm that can process a lot of data at one time is required to solve the problem, one of them is Naïve Bayes algorithm. One of Naïve Bayes weaknesses is its accuracy that depends on how many attributes of the data being used. Therefore, the Particle Swarm Optimization algorithm is used as attributes reduction algorithm, and also enhance Naïve Bayes's accuracy. The accuracy result of Naïve Bayes is 91,55% and Naïve Bayes optimized with Particle Swarm Optimization is 99,13%, resulting accuracy enhancement by 7,58%.

Keywords : Naïve Bayes, Particle Swarm Optimzation, DDoS, Classification.

Palembang, Juli 2020

Pembimbing I

Dian Palupi Rini, M.Kom., Ph.D.
NIP. 197802232006042002

Pembimbing II

Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Mengetahui,
Ketua Jurusan Teknik Informatika,

Rifkie Primartha, M.T
NIP. 197706012009121004

OPTIMASI NAIVE BAYES UNTUK KLASIFIKASI SERANGAN DDOS DENGAN PARTICLE SWARM OPTIMIZATION

Oleh :
Cokro Nurwinto
09021381520079

ABSTRAK

DDoS adalah salah satu jenis serangan internet / dunia maya yang berbahaya. Salah satu solusi untuk menanggulangi masalah tersebut adalah dengan cara mengidentifikasi suatu trafik jaringan apakah mengandung serangan DDoS atau tidak. Identifikasi memerlukan data yang cukup agar dapat mengenali pola dari DDoS agar dapat dicegah sesegera mungkin. Namun, dikarenakan jumlah data trafik jaringan yang sangat banyak per-detiknya, digunakan algoritma klasifikasi untuk mengatasi masalah tersebut. Salah satu algoritma klasifikasi yang mampu menangani banyak data sekaligus adalah algoritma Naïve Bayes. Salah satu kelemahan dari Naïve Bayes adalah ketergantungan hasil akurasi yang dihasilkan berdasarkan banyak atribut yang digunakan, oleh karena itu digunakan algoritma Particle Swarm Optimization (PSO) sebagai algoritma optimasi guna mengurangi pemakaian atribut dan meningkatkan akurasi dari algoritma Naïve Bayes. Dari pengujian, didapat hasil akurasi dari Naïve Bayes saja sebesar 91,55% dan Naïve Bayes yang dioptimasi dengan Particle Swarm Optimization sebesar 99,13%. Didapat peningkatan akurasi yang didapat sebesar 7,58%.

Kata kunci : *Naïve Bayes, Particle Swarm Optimzation*, DDoS, Klasifikasi.

Palembang, Juli 2020

Pembimbing I

Dian Palupi Rini, M.Kom., Ph.D.
NIP. 197802232006042002

Pembimbing II

Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Mengetahui,
Ketua Jurusan Teknik Informatika,

Rifkie Primartha, M.T
NIP. 197706012009121004

KATA PENGANTAR

bismillaahirrahmaanirrahiim

Puji syukur kepada Allah swt atas berkat serta rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas akhir ini disusun untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 di Fakultas Ilmu Komputer Universitas Sriwijaya.

Dalam menyelesaikan Tugas Akhir ini, banyak pihak telah memberikan bantuan dan dukungan, baik secara langsung maupun secara tidak langsung. Oleh karenanya, Penulis ingin berterima kasih kepada :

1. Allah swt, karena kalau bukan karena izin-Nya, penulis tidak akan dapat menyelesaikan Tugas Akhir ini dengan baik.
2. Kedua Orang tua, Winoto Chandra dan R.A. Susilawati, adikku, Ahmad Dwitanto, nyaiku R.A. Zuhria, serta seluruh keluargaku yang mendoakan serta memberikan dukungan baik secara materil maupun moral.
3. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya, Bapak Rifkie Primartha, M.T. selaku Ketua Jurusan Teknik Informatika, dan Ibu Alvi Syahrini Utami, M.Kom., selaku Sekretaris Jurusan Teknik Informatika.
4. Ibu Dian Palupi Rini, M.Kom., Ph.D., selaku Dosen Pembimbing I dan Bapak Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing II yang telah membimbing, memotivasi dan memberi arahan kepada Penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
5. Bapak Osvari Arsalan, S.Kom., M.T., selaku Dosen Pembimbing Akademik, yang telah membimbing dan mengarahkan serta memotivasi Penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
6. Ibu Yunita, M.Cs., selaku Dosen Penguji I dan Bapak Danny Matthew Saputra, M.Sc., selaku Dosen Penguji II yang telah memberi masukan dan dorongan dalam proses pengerjaan Tugas Akhir.

7. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Mba Wiwin, Pak Toni, dan seluruh staf tata usaha yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.
9. Sahabat-sahabat ku (Annis, Husni, Ilham S, Raka, Robert, Salim) yang selalu memberikan motivasi pada Penulis selama masa perkuliahan dan pengerjaan Tugas Akhir.
10. Teman-teman seperjuangan (Adi, Agus, Ajrul, Alex, Gheddi, Hanif, Ilham) dalam pengerjaan Tugas Akhir dan teman-teman seperjuangan yang telah lulus mendahului Penulis (Abiyyu, Imam, Opan, Rusdi), yang kadang dan selalu datang ke basecamp dan party sampai bosan, yang telah mendampingi dan memberikan banyak bantuan kepada Penulis dalam proses pengerjaan Tugas Akhir.
11. Teman-teman IFBIL A 2015 dan seluruh teman-teman Teknik Informatika Universitas Sriwijaya.

Penulis menyadari bahwa dalam penyusunan Tugas Akhir ini masih banyak sekali kekurangan disebabkan kurangnya pengalaman dan pengetahuan. Oleh karena itu Penulis mengharapkan saran dan kritik yang membangun guna kemajuan penelitian selanjutnya. Akhir kata, semoga Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, Juli 2020

Cokro Nurwinto

DAFTAR ISI

Halaman

HALAMAN JUDUL i
LEMBAR PENGESAHAN TUGAS AKHIR ii
TANDA LULUS UJIAN SIDANG TUGAS AKHIR iii
HALAMAN PERNYATAAN iv
MOTTO DAN PERSEMBAHAN v
ABSTRACT vi
ABSTRAK vii
KATA PENGANTAR viii
DAFTAR ISI x
DAFTAR TABEL xv
DAFTAR GAMBAR xviii
DAFTAR LAMPIRAN xx

BAB I PENDAHULUAN
1.1. Pendahuluan I-1
1.2. Latar Belakang Masalah I-1
1.3. Rumusan Masalah I-4
1.4. Tujuan Penelitian I-5
1.5. Manfaat Penelitian I-5
1.6. Batasan Masalah I-5
1.7. Sistematika Penulisan I-6
1.8. Kesimpulan I-8

BAB II KAJIAN LITERATUR
2.1. Pendahuluan II-1
2.2. *Distributed Denial of Service* (DDoS) II-1
2.2.1. Karakteristik DDoS II-1

2.2.2. Metode Serangan DDoS II-2
2.3. Praproses II-5
2.3.1. Normalisasi II-5
2.4. *Naïve Bayes* II-6
2.5. *Particle Swarm Optimization* (PSO) II-6
2.6. *Naïve Bayes* berbasis *Particle Swarm Optimization* (*Naïve Bayes* – PSO) II-7
2.7. *Confusion Matrix* II-10
2.8. *Rational Unified Process* (RUP) II-11
2.9. Penelitian Lain Yang Relevan II-13
2.10. Kesimpulan II-17

BAB III METODOLOGI PENELITIAN
3.1. Pendahuluan III-1
3.2. Pengumpulan Data III-1
. 3.2.1. Jenis dan Sumber Data III-1
. 3.2.2. Metode Pengumpulan Data III-1
3.3. Tahapan Penelitian III-2
3.3.1. Menetapakan Kerangka Kerja / *Framework* III-3
3.3.2. Menetapkan Kriteria Pengujian III-3
3.3.3. Menetapkan Format Pengujian III-3
3.3.4. Menentukan Alat yang Digunakan dalam Pelaksanaan Penelitian III-6
3.3.5. Melakukan Pengujian Penelitian III-6
3.3.6. Melakukan Analisa Hasil Pengujian dan Membuat Kesimpulan Penelitian III-7
3.4. Metode Pengembangan Perangkat Lunak III-7
3.4.1. Fase Insepsi III-7
3.4.2. Fase Elaborasi III-8
3.4.3. Fase Konstruksi III-8
3.4.4. Fase Transisi III-9

3.5. Manajemen Proyek Penelitian III-9
3.6. Kesimpulan III-22

BAB IV PENGEMBANGAN PERANGKAT LUNAK
4.1. Pendahuluan IV-1
4.2. *Rational Unified Process* (RUP) IV-1
4.2.1. Fase Insepsi IV-1
4.2.1.1. Pemodelan Bisnis IV-1
4.2.1.2. Kebutuhan Sistem IV-3
4.2.1.3. Analisis dan Desain IV-5
4.2.1.3.1. Analisis Kebutuhan Perangkat Lunak ... IV-5
4.2.1.3.2. Analisis Data IV-6
4.2.1.3.3. Analisis Praproses IV-7
4.2.1.3.4. Analisis Algoritma *Naive Bayes* IV-9
4.2.1.3.5. Analisis Metode *Particle Swarm Optimization* IV-13
4.2.1.4. Desain Perangkat Lunak IV-16
4.2.2. Fase Elaborasi IV-22
4.2.2.1. Pemodelan Bisnis IV-22
4.2.2.1.1. Perancangan Data IV-22
4.2.2.1.2. Perancangan Antarmuka IV-22
4.2.2.2. Kebutuhan Sistem IV-23
4.2.2.3. Diagram IV-23
4.2.2.3.1. *Activity Diagram* IV-24
4.2.2.3.2. *Sequence Diagram* IV-27
4.2.3. Fase Konstruksi IV-28
4.2.3.1. Kebutuhan Sistem IV-28
4.2.3.2. Class Diagram IV-29
4.2.3.3. Kelas Analisis IV-30
4.2.3.4. Implementasi IV-31
4.2.3.4.1. Implementasi Kelas IV-31

4.2.3.4.2. Implementasi Antarmuka IV-33
4.2.4. Fase Transisi IV-33
4.2.4.1. Pemodelan Bisnis IV-33
4.2.4.2. Kebutuhan Sistem IV-34
4.2.4.3. Rencana Pengujian IV-34
4.2.4.3.1. Rencana Pengujian *Use Case* Memuat Data IV-34
4.2.4.3.2. Rencana Pengujian *Use Case* Klasifikasi DDoS dengan *Naive Bayes* .. IV-35
4.2.4.3.3. Rencana Pengujian *Use Case* Klasifikasi DDoS dengan *Naive Bayes* + PSO IV-35
4.2.4.4. Implementasi IV-36
4.2.4.4.1. Pengujian *Use Case* Memuat Data IV-37
4.2.4.4.2. Pengujian *Use Case* Klasifikasi DDoS dengan Naive Bayes IV-37
4.2.4.4.3. Pengujian *Use Case* Klasifikasi DDoS dengan Naive Bayes + PSO IV-38
4.3. Kesimpulan IV-40

BAB V HASIL DAN ANALISIS PENELITIAN
5.1. Pendahuluan V-1
5.2. Data Hasil Percobaan / Penelitian V-1
5.2.1. Konfigurasi Percobaan V-1
5.2.2. Data Hasil Konfigurasi V-2
5.2.2.1. Hasil Pengujian Konfigurasi I V-3
5.2.2.2. Hasil Pengujian Konfigurasi II V-5
5.2.2.3. Hasil Pengujian Konfigurasi III V-6
5.3. Analisis Hasil Pengujian …… V-9
5.4. Kesimpulan V-10

BAB VI KESIMPULAN DAN SARAN
6.1 Pendahuluan VI-1
6.2 Kesimpulan VI-1
6.3. Saran VI-2
DAFTAR PUSTAKA …….. xxi
DAFTAR LAMPIRAN …… xxiii

DAFTAR TABEL

		Halaman
Tabel II-1	Penelitian Lain yang Relevan ……..……..	II-15
Tabel III-1	Rancangan Tabel Konfigurasi Pengujian Berdasarkan Perubahan Jumlah Iterasi Maksimum ……...	III-4
Tabel III-2	Rancangan Tabel Konfigurasi Pengujian Berdasarkan Perubahan Jumlah Populasi Maksimum ……..…..	III-5
Tabel III-3	Rancangan Tabel Konfigurasi Pengujian Berdasarkan Perubahan Jumlah *Learning Rate* Maksimum ……..….	III-5
Tabel III-4	Penjadwalan Penelitian dalam Bentuk *Work Breakdown Structure* (WBS) …….……..	III-10
Tabel IV-1	Kebutuhan Fungsional ……..	IV-4
Tabel IV-2	Kebutuhan Non-Fungsional ……..	IV-5
Tabel IV-3	Contoh Data *Traffic* Jaringan ……	IV-7
Tabel IV-4	Nilai *Median* Contoh Data *Traffic* Jaringan ……..	IV-8
Tabel IV-5	Normalisasi Contoh Data *Traffic* Jaringan ……	IV-8
Tabel IV-6	Frekuensi Kemunculan Data Tiap Atribut ……	IV-10
Tabel IV-7	Parameter PSO ……..	IV-14
Tabel IV-8	Nilai *Fitness* Tiap Partikel ……	IV-15
Tabel IV-9	Definisi Aktor ……...	IV-17
Tabel IV-10	Definisi *Use Case* …….	IV-18
Tabel IV-11	Skenario *Use Case* Memuat Data ……..	IV-19
Tabel IV-12	Skenario *Use Case* Klasifikasi DDoS dengan *Naive Bayes* ……..	IV-20

Tabel IV-13	Skenario *Use Case* Klasifikasi DDoS dengan *Naive Bayes* + PSO …….	IV-21
Tabel IV-14	Kebutuhan Sistem …….	IV-23
Tabel IV-15	Implementasi Kelas ……..	IV-34
Tabel IV-16	Kebutuhan Sistem …….	IV-34
Tabel IV-17	Rencana Pengujian *Use Case* Memuat Data …….	IV-34
Tabel IV-18	Rencana Pengujian *Use Case* Klasifikasi DDoS dengan *Naive Bayes* ……..	IV-35
Tabel IV-19	Rencana Pengujian *Use Case* Klasifikasi DDoS dengan *Naive Bayes* + PSO ……...	IV-35
Tabel IV-20	Pengujian *Use Case* Memuat Data ……	IV-37
Tabel IV-21	Pengujian *Use Case* Klasifikasi DDoS dengan *Naive Bayes* ……	IV-37
Tabel IV-22	Pengujian *Use Case* Klasifikasi DDoS dengan *Naive Bayes* + PSO …….	IV-38
Tabel V-1	Hasil Klasifikasi Naive Bayes ....……....	V-2
Tabel V-2	Hasil Pengujian Tabel Konfigurasi Pengujian I Berdasarkan Perubahan Jumlah Iterasi Maksimum ….....	V-3
Tabel V-3	Hasil Pengujian Tabel Konfigurasi Pengujian I Hasil Klasifikasi	V-4
Tabel V-4	Pengujian Tabel Konfigurasi Pengujian II Berdasarkan Perubahan Jumlah Partikel Maksimum	V-5

Tabel V-5 Pengujian Tabel Konfigurasi Pengujian II Hasil Klasifikasi V-5
Tabel V-6 Hasil Pengujian Tabel Konfigurasi Pengujian III Berdasarkan Perubahan Jumlah *Learning Rate* Maksimum V-7
Tabel V-7 Hasil Pengujian Tabel Konfigurasi Pengujian III Hasil Klasifikasi V-7
Tabel V-8 Hasil Pengujian Perbandingan Nilai Akurasi V-9
Tabel V-9 Hasil Pengujian Perbandingan Hasil Klasifikasi V-10

DAFTAR GAMBAR

Halaman

Gambar II-1	Ilustrasi Serangan DDoS ……..……	II-3
Gambar II-2	Arsitektur *Rational Unified Process* ……...…..	II-11
Gambar III-1	Tahapan Penelitian ……..	III-2
Gambar III-2	Tahapan Pengujian Penelitian .....…….	III-6
Gambar III-3	Penjadwalan Penelitian Tahap Menentukan Ruang Lingkup dan Unit Penelitian	III-19
Gambar III-4	Penjadwalan Penelitian Tahap Menentukan Dasar Teori yang Berkaitan dengan Penelitian ……...	III-19
Gambar III-5	Penjadwalan Penelitian Tahap Menentukan Kriteria Pengujian ……..	III-20
Gambar III-6	Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian pada Fase Insepsi ……..	III-20
Gambar III-7	Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian pada Fase Elaborasi ……..	III-20
Gambar III-8	Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian pada Fase Konstruksi ……	III-21
Gambar III-9	Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian pada Fase Transisi …….	III-22
Gambar III-10	Penjadwalan Penelitian Tahap Melakukan Pengujian Penelitian ……..	III-23
Gambar III-11	Penjadwalan Penelitian Tahap Melakukan Analisa Hasil Pengujian dan Membuat Kesimpulan ……..	III-23
Gambar IV-1	Diagram *Use Case* Perangkat Lunak	IV-17

Gambar IV-2	Diagram Aktivitas *Use Case* Klasifikasi DDoS dengan *Naive Bayes* + PSO ……...	IV-22
Gambar IV-3	*Activity Diagram Use Case* Memuat Data ……	IV-24
Gambar IV-4	*Activity Diagram Use Case* Klasifikasi DDoS dengan *Naive Bayes* ……..	IV-25
Gambar IV-5	*Activity Diagram Use Case* Klasifikasi DDoS dengan *Naive Bayes* + PSO ……...	IV-26
Gambar IV-6	*Sequence Diagram Use Case* Memuat Data ……	IV-27
Gambar IV-7	*Sequence Diagram Use Case* Klasifikasi DDoS dengan *Naive Bayes* ……..	IV-27
Gambar IV-8	*Sequence Diagram Use Case* Klasifikasi DDoS dengan NB + PSO …….	IV-28
Gambar IV-9	*Class Diagram* …….	IV-29
Gambar IV-10	Kelas Analisis Memilih Berkas ……	IV-30
Gambar IV-11	Kelas Analisis Melakukan Klasifikasi *Naive Bayes* …	IV-30
Gambar IV-12	Kelas Analisis Melakukan Klasifikasi *Naive Bayes* + PSO ……..	IV-31
Gambar IV-13	Implementasi Antarmuka …….	IV-33

DAFTAR LAMPIRAN

		Halaman
Lampiran-1	Atribut Dataset Friday Working Hours ……	L-1
Lampiran-2	*Source Code* Program ……..……	L-2

BAB I

PENDAHULUAN

1.1. Pendahuluan

Pada bab ini akan menjelaskan tentang pembahasan umum penelitian yaitu, latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, Batasan masalah serta uraian singkat bab per bab dalam penelitian ini.

1.2. Latar Belakang Masalah

Sejak awal kemunculuannya, internet menjadi fenomena baru pada saat itu. Dengan adanya internet, terciptalah teknologi-teknologi baru yang mempremudah manusia dalam melakukan kegiatan mereka sehari-hari sehingga, internet menjadi sebuah candu bagi pendunggunanya. Namun, dibalik kemudahan yang didapat, terdapat juga resiko yang perlu diperhatikan oleh pengguna internet, salah satunya adalah tentang ancaman serangan *cyber* yang bisa datang kapan saja, mengingat masih banyak pengguna internet yang masih kurang memperhatikan faktor keamanan dalam penjelajahan internet secara *online*. *Distributed Denial of Service* (DDoS) merupakan salah satu ancaman dalam keamanan *cyber*. Menurut laporan peneliti Kaspersky Oleg, Badovskaya, & Gutnikov (2019), DDoS merupakan ancaman *cyber* yang berbahaya dan masih marak digunakan hingga sekarang. Dilaporkan terjadi peningkatan penggunaan serangan jenis ini pada kuartal ke-2 tahun 2018 sampai kuartal ke-2 tahun 2019 yang meningkat sebesar 46%.

Akibat dari ini tidak main-main, hal ini dibuktikan dengan kerusakan yang dihasilkan dari serangan tersebut, yaitu komputer atau jaringan komputer yang tidak dapat menyediakan layanan secara normal. DDoS melancarkan serangannya pada jaringan dengan volume *traffic bandwith* yang tinggi sehingga, semua *resources* yang ada akan tidak tersedia (Hermawan, 2013). Oleh karena itu diperlukan suatu cara agar dapat mengidentifikasi suatu *traffic* jaringan, yaitu dengan cara melakukan proses klasifikasi pada data *traffic* tersebut untuk mengetahui apakah ia merupakan *traffic* serangan atau bukan.

Dikarenakan jumlah data *traffic network* yang banyak per-detiknya, maka dibutuhkan suatu algoritma klasifikasi yang dapat mengklasifikasikan suatu data yang banyak dalam waktu yang singkat. Diantara banyaknya algoritma klasifikasi, *Naïve Bayes* dinilai cocok untuk digunakan dalam penelitian ini. *Naïve Bayes* memiliki kecepatan dan ketepatan yang tinggi untuk proses klasifikasi walaupun data yang dipakai bervolume besar. Namun dibalik keunggulannya, *Naïve Bayes* memiliki kelemahan yang perlu diperhatikan, yaitu ketergantungan hasil akurasi yang dihasilkan berdasarkan banyaknya atribut atau variabel yang digunakan (Muhamad et al., 2017).

Pada penelitian sebelumnya, Wirawan & Eksistyanto (2015) melakukan proses klasifikasi dengan menggunakan algoritma *Naïve Bayes* dengan metode diskritisasi dalam penerapan *Intrusion Detection System* (IDS) mendapat hasil akurasi sebesar 59,6% tanpa proses diskritisasi dan 89,10% dengan proses

diskritisasi. Fadlil, Riadi, & Aji (2017) menggunakan *Naïve Bayes* dengan metode *Gaussian* dalam klasifikasi dan mendapat nilai akurasi sebesar 100%, namun hasil yang tinggi tersebut dapat diperoleh dikarenakan data uji yang digunakan telah melalui tahap pra-proses secara manual terlebih dahulu. Dari hasil penelitian-penelitian yang telah didapat tersebut menunjukan bahwa algoritma *Naive Bayes* membutuhkan algoritma pendukung guna menutupi kekurangan pada *Naïve Bayes* yang telah disinggung sebelumnya.

Untuk menutupi kelemahan yang ada pada *Naïve Bayes*, *Particle Swarm Optimization* (PSO) dinilai cocok untuk digunakan. PSO memiliki beberapa keunggulan, yaitu tidak ada evolusi pada operatornya, penerapannya yang mudah serta penggunaan parameternya yang sedikit. Selain itu bila dibandingkan dengan metode heuristic lainnya seperti Algoritma Genetika, PSO lebih fleksibel dalam menjaga keseimbangan antara pencarian global dan local terhadap *search space*-nya (Sathya & Kayalvizhi, 2010). Sistem pada PSO sendiri diinisiasi oleh sebuah populasi solusi acak dan selanjutnya mencari titik optimum dengan cara meng-*update* tiap hasil dari pembangkitan populasi. (Widiastuti et al., 2014). Dengan digunakannya algoritma PSO dalam optimasi, diharapkan akan menambah akurasi dari algoritma *Naïve Bayes.*

(Ernawati, 2016) melakukan seleksi fitur pada *Sentiment Analysis Review* dengan *Particle Swarm Optimization*. Peningkatan akurasi yang didapat sebesar

7,38%, dari 79,50% sampai dengan 86,88%. Hasil tersebut menunjukan bahwa algoritma PSO dapat digunakan untuk mengoptimasi algoritma *Naïve Bayes*.

Berdasarkan uraian di atas, pada penelitian ini akan dilakukan pengklasifikasian menggunakan algoritma *Naïve Bayes* yang diharapkan dapat digunakan untuk melakukan klasifikasi mana dan mana yang bukan, dan menggunakan *Particle Swarm Optimization* yang diharapkan dapat digunakan untuk mengoptimasi algoritma *Naïve Bayes* dalam melakukan pengklasifikasian .

1.3. Rumusan Masalah

Berdasarkan latar belakang yang dikemukakan diatas, adapun rumusan masalah dalam penelitian ini ialah tingkat akurasi yang dihasilkan oleh Algoritma *Naïve Bayes* yang di optimasi dengan *Particle Swarm Optimization* (PSO). Berdasarkan rumusan masalah, maka pertanyaan penelitian yang didapat adalah :

1. Bagaimana hasil seleksi fitur yang paling optimal dari algoritma *Naïve Bayes* yang di optimasi dengan *Particle Swarm Optimization* dalam pengklasifikasian *data traffic network* ?

2. Bagaimana hasil klasifikasi dari algoritma *Naïve Bayes* yang dioptimasi dengan *Particle Swarm Optimization* dalam pengklasifikasian *data traffic network*?

1.4. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Untuk mengetahui hasil seleksi fitur yang paling optimal dari algoritma *Naïve Bayes* yang di optimasi dengan *Particle Swarm Optimization* dalam pengklasifikasian *data traffic network*
2. Untuk mengetahui hasil klasifikasi dari penerapan algoritma *Naïve Bayes* yang dioptimasi dengan *Particle Swarm Optimization* dalam pengklasifikasian *data traffic network.*

1.5. Manfaat Penelitian

Adapun manfaat penelitian ini adalah :

1. Memahami pengaruh dari algoritma *Particle Swarm Optimization* dalam peningkatan akurasi dari algoritma *Naïve Bayes*.
2. Memahami penerapan algoritma *Particle Swarm Optimization* pada *Naïve Bayes* untuk klasifikasi data *traffic network.*

1.6.Batasan Masalah

Adapun batasan masalah penelitian ini adalah :

1. Hanya membahas serangan *Distributed Denial of Service* (DDoS) secara umum.
2. Tidak membahas tentang pencegahan dan pendeteksian DDoS, melainkan terbatas pada klasifikasi saja.

3. Dataset bersifat *public* dan berupa data *packet traffic network* normal dan *traffic network* serangan yang telah dikonversi menjadi file.*xlsx*
4. Jumlah data yang digunakan sebanyak 8000 data untuk data latih dan 2000 data untuk data uji.

1.7.Sistematika Penulisan

Untuk memahami lebih jelas proposal penelitian ini, pemaparan materi dikelpompokkan menjadi beberapa bab dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang, tujuan penelitian, manfaat penelitian, Batasan masalah dan sistematika penulisan.

BAB II KAJIAN LITERATUR

Bab ini akan membahas dasar teori yang digunakan dalam penelitian, seperti *Distributed Denial of Service* (DDoS), *Naïve Bayes*, *Particle Swarm Optimization* (PSO), *Confusion Matrix* dan *Rational Unified Process* (RUP). Pada akhir bab akan disertakan penelitian-penelitian yang relevan terkait dengan penelitian ini.

BAB III METODOLOGI PENELITIAN

Bab ini akan membahas tahapan yang akan dilaksanakan pada penelitian ini. Masing-masing rencana tahapan penelitian dideskripsikan dengan rinci dengan mengacu pada suatu kerangka kerja. Di akhir bab ini berisi perancangan manajemen proyek pada pelaksanaan penelitian.

BAB IV PENGEMBANGAN PERANGKAT LUNAK

Bab ini akan membahas perancangan dan implementasi perangkat lunak dengan metode pemrograman berorientasi objek berdasarkan panduan RUP yang di dalamnya terdapat 4 fase, yaitu insepsi, elaborasi, konstruksi, dan transisi.

BAB V HASIL DAN ANALISIS PENELITIAN

Bab ini akan membahas hasil klasifikasi algoritma *Naïve Bayes* dan hasil optimasinya dengan menggunakan *Particle Swarm* Optimization. Pada akhir bab berisi analisis dari hasil yang telah didapat.

BAB VI KESIMPULAN DAN SARAN

Bab ini akan membahas kesimpulan dan saran berdasarkan hasil analisis dalam meningkatkan akurasi algoritma *Naïve Bayes* dengan menggunkan *Particle Swarm Optimization* pada pengklasifikasian .

1.8.Kesimpulan

Berdasarkan uraian diatas, pada penelitian ini akan dilakukan optimasi algorima *Naïve Bayes* dengan *Particle Swarm Optimization* terhadap dengan batasan masalah yang telah ditentukan.

DAFTAR PUSTAKA

Aulianita, R., & Rifai, A. (2018). Optimasi Particle Swarm Optimization pada Naive Bayes untuk Sentiment Analysis Furniture. *Information Management for Educators and Professionals*, *3*(1), 31–40.

Ernawati, S. (2016). *Penerapan Particle Swarm Optimization Untuk Seleksi Fitur Pada Analisis Sentimen Review Perusahaan Penjualan Online Menggunakan Naïve Bayes*. *2015*(June), 50061.

Fadlil, A., Riadi, I., & Aji, S. (2017). DDoS Attacks Classification using Numeric Attribute-based Gaussian Naive Bayes. *International Journal of Advanced Computer Science and Applications*, *8*(8). https://doi.org/10.14569/ijacsa.2017.080806

Fibrianda, M. F., & Bhawiyuga, A. (2018). Analisis Perbandingan Akurasi Deteksi Serangan pada Jaringan Komputer dengan Metode Naïve Bayes dan Support Vector Machine (SVM). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *2*(9), 3112–3123.

Geges, S., & Wibisono, W. (2015). Pengembangan Pencegahan Serangan Distributed Denial of Service (DDoS) pada Sumber Daya Jaringan dengan Integrasi Network Behavior Analysis dan Client Puzzle. *JUTI: Jurnal Ilmiah Teknologi Informasi*, *13*(1), 53. https://doi.org/10.12962/j24068535.v13i1.a388

Hermawan, R. (2013). Analisis Konsep dan Cara Kerja Serangan Komputer Distributed Denial of Service (DDoS). *Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)*, *5*(1), 1–14.

Kotsiantis, S. B., Kanellopoulos, D., & Pintelas, P. E. (2007). *Microsoft Word - Abdelouahab Moussaoui.doc - data-preprocessing-for-supervised-leaning*. *1*(12), 4091–4096. http://waset.org/publications/14136/data-preprocessing-for-supervised-leaning

Li, J., Ding, L., & Li, B. (2014). A Novel Naive Bayes Classification Algorithm

Based On Particle Swarm Optimization. *Open Automation and Control Systems Journal*, *6*(1), 747–753. https://doi.org/10.2174/1874444301406010747

Manalil, J. (2010). Rational Unified Process. *Computer*, *August*.

Menarianti, I. (2015). Klasifikasi Data Mining dalam Menentukan Pemberian Kredit Bagi Nasabah Koperasi. *Jurnal Ilmiah Teknosains*, *1*(1), 1–10.

Muhamad, H., Prasojo, C. A., Sugianto, N. A., Surtiningsih, L., & Cholissodin, I. (2017). Optimasi Naïve Bayes Classifier dengan Menggunakan Particle Swarm Optimization pada Data Iris. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *4*(3), 180. https://doi.org/10.25126/jtiik.201743251

Nasution, D. A., Khotimah, H. H., & Chamidah, N. (2019). Perbandingan Normalisasi Data untuk Klasifikasi Wine Menggunakan Algoritma K-NN. *Computer Engineering, Science and System Journal*, *4*(1), 78. https://doi.org/10.24114/cess.v4i1.11458

Oleg, K., Badovskaya, E., & Gutnikov, A. (2019). *DDoS attacks in Q2 2019*. https://securelist.com/ddos-report-q2-2019/91934/

Primartha, R., Adhi Tama, B., Arliansyah, A., & Januar Miraswan, K. (2019). Decision Tree Combined with PSO-Based Feature Selection for Sentiment Analysis. *Journal of Physics: Conference Series*, *1196*(1). https://doi.org/10.1088/1742-6596/1196/1/012018

Sathya, P. D., & Kayalvizhi, R. (2010). PSO-Based Tsallis Thresholding Selection Procedure for Image Segmentation. *International Journal of Computer Applications*, *5*(4), 39–46. https://doi.org/10.5120/903-1279

Xue, B., Zhang, M., & Browne, W. N. (2013). Particle Swarm Optimization for Feature Selection in Classification: A Multi-Objective Approach. *IEEE Transactions on Cybernetics*. https://doi.org/10.1109/TSMCB.2012.2227469