

**IMPLEMENTASI *PRINCIPAL COMPONENT ANALYSIS* (PCA)  
DAN ALGORITMA *NAÏVE BAYES CLASSIFIER* PADA  
KLASIFIKASI *BOTNET* DI JARINGAN *INTERNET OF  
THINGS* (IoT)**

**TUGAS AKHIR**



**Oleh:**

**Widyana Aprianti  
09011181621010**

**JURUSAN SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SRIWIJAYA  
2021**

**IMPLEMENTASI PRINCIPAL COMPONENT ANALYSIS (PCA)  
DAN ALGORITMA NAÏVE BAYES CLASSIFIER PADA  
KLASIFIKASI BOTNET DI JARINGAN INTERNET OF  
THINGS (IoT)**

**TUGAS AKHIR**

**Diajukan Untuk Melengkapi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer (S1)**



**Oleh:**

**Widyana Aprianti  
09011181621010**

**JURUSAN SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SRIWIJAYA  
2021**

**LEMBAR PENGESAHAN**  
**IMPLEMENTASI *PRINCIPAL COMPONENT ANALYSIS (PCA)***  
**DAN ALGORITMA *NAÏVE BAYES CLASSIFIER* PADA**  
**KLASIFIKASI BOTNET DI JARINGAN *INTERNET OF***  
***THINGS (IoT)***

**TUGAS AKHIR**

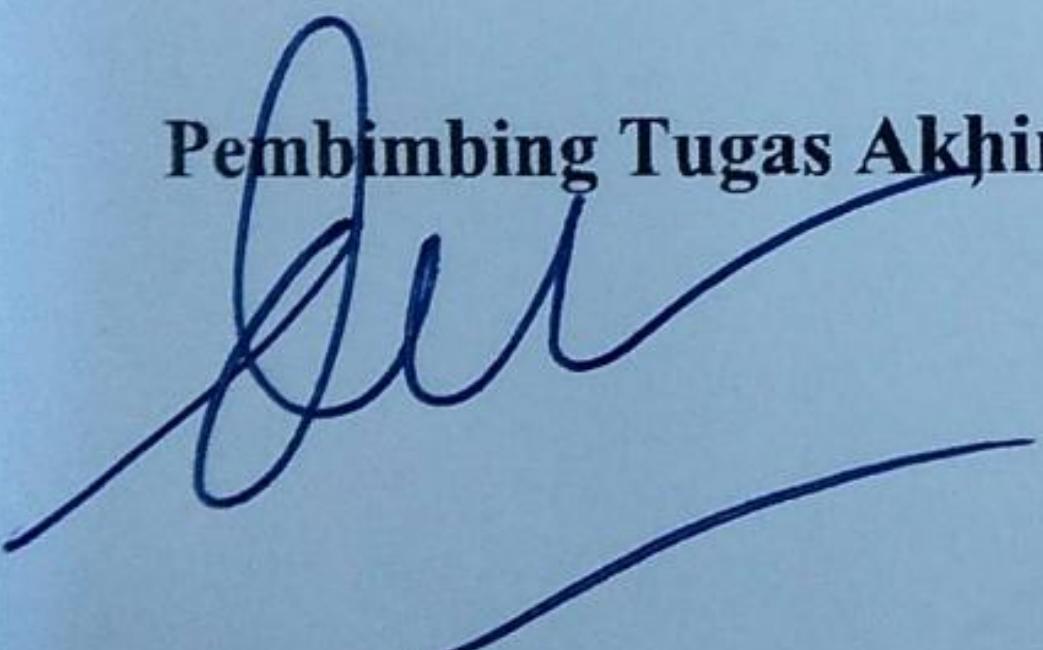
**Diajukan Untuk Melengkapi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer**

**Oleh :**

**WIDYANA APRIANTI  
09011181621010**

**Indralaya, Juli 2021**

Pembimbing Tugas Akhir



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

Mengetahui,  
Ketua Jurusan Sistem Komputer



Dr. Ir. H. Sukemi, M.T.  
NIP. 199612032006041001

## HALAMAN PERSETUJUAN

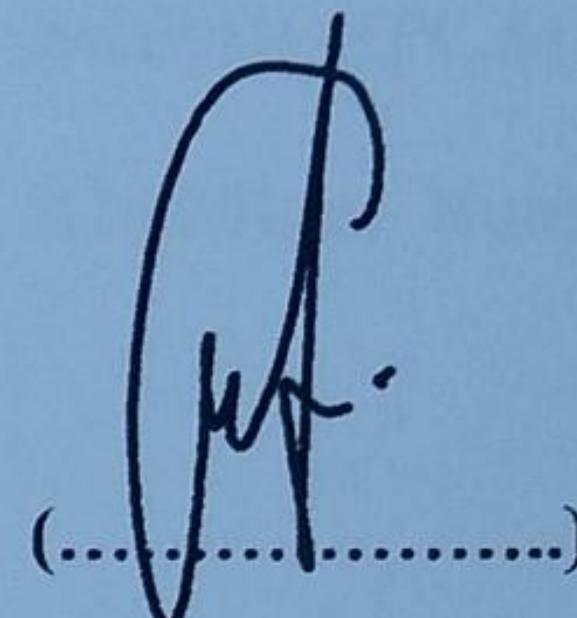
Telah Diuji dan lulus pada :

Hari : Jumat

Tanggal : 2 Juli 2021

**Tim Penguji:**

1. Ketua : Ahmad Zarkasi, M.T.



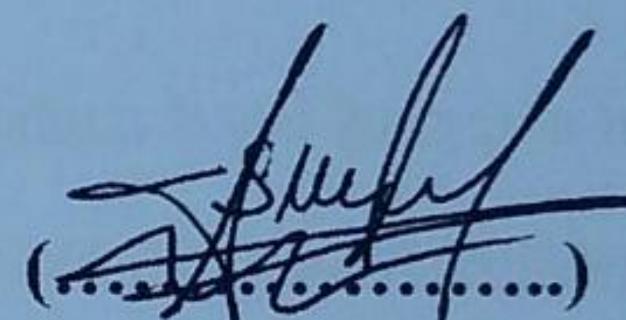
(.....)

2. Sekretaris : Rendyansyah, M.T.



(.....)

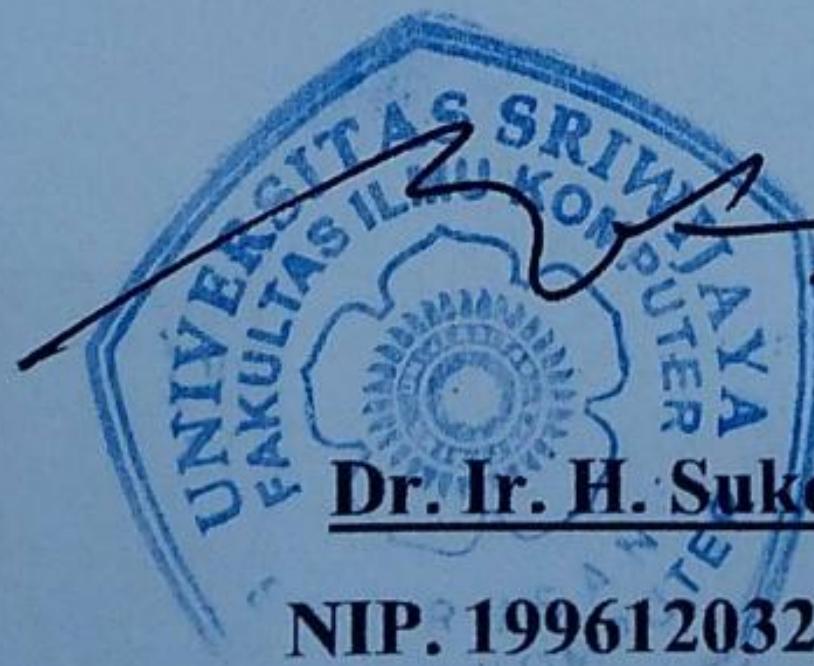
3. Penguji : Sarmayanta Sembiring, M.T.



(.....)

**Mengetahui,**

**Ketua Jurusan Sistem Komputer**



Dr. Ir. H. Sukemi, M.T.

NIP. 199612032006041001

## HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

**Nama : Widyana Aprianti**

**NIM : 09011181621010**

**Judul : Implementasi Principal Component Analysis (PCA) dan Algoritma Naive Bayes Classifier Pada Klasifikasi Botnet di Jaringan Internet of Things (IoT)**

Hasil Penggecekan Software iThenticate/Turitin : 10%

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

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan

Indralaya, Juni 2021



Widyana Aprianti

NIM. 09011181621010

## **HALAMAN PERSEMBAHAN**

**Kutipan :**

*“Allah Tidak Membebani Seseorang Melainkan Sesuai Dengan  
Kesanggupannya”  
(Q.S Al-Baqarah : 286)*

*“Maka Nikmat Tuhan-mu Yang Manakah Yang Kamu Dustakan?”  
(Q.S Ar-Rahman : 13)*

*“Ibuk Ayah Maaf Ayuk Baru Bisa Selesai Sekarang”*

*“Maaf Dek Tahun Ini Kamu Istirahat Dulu, Tahun Depan Kita Gas”*

**Tugas Akhir Ini Saya Persembahkan Untuk :**

- Allat SWT
- Ibu Maryana dan Ayah Danial tercinta yang senantiasa selalu menjadi penyemangat serta menyertai setiap urusan saya.
- Adik kandung saya Nadia Rupa Dalena yang selalu sabar menghadapi kepusingan saya selama menjalani perskripsian.
- Keluarga besar dari pihak dan Ibu dan Ayah yang selalu mendoakan dan memberi dukungan kepada saya.
- My best partner yang selalu mendoakan dan memberi dukungan kepada saya.
- Sahabat - sahabat saya yang selalu mendoakan dan memberi dukungan kepada saya.
- Teman – teman seperjuangan di Sistem Komputer 2016.
- Jurusan Sistem Komputer
- Almamater

## KATA PENGANTAR

Puji syukur atas kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan Tugas Akhir ini dengan judul “**Implementasi Principal Component Analysis (PCA) dan Algoritma Naïve Bayes Classifier Pada Klasifikasi Botnet di Jaringan Internet of Things (IoT)**”.

Penulisan Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan tugas akhir ini. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Kedua Orang Tua Ibu (Maryana) dan Ayah (Danial) serta adik kandung saya (Nadia Rupa Dalena) yang telah memberikan doa dan restu serta dukungan yang sangat besar selama mengikuti dan melaksanakan perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya hingga dapat menyelesaikan Tugas Akhir ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Huda Ubaya, MT. selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph.D selaku Dosen Pembimbing Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

6. Mbak Nurul Afifah, S.Kom, M.Kom yang telah sangat membantu saya dalam penulisan Tugas Akhir ini.
7. Abdi Bimantara, S.Kom yang telah sangat membantu saya dalam penulisan Tugas Akhir ini.
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Mbak Renny Virgasari selaku Admin Jurusan Sistem Komputer yang telah membantu administrasi dalam menyelesaikan Tugas Akhir.
10. Kakak - kakak tingkat yang menjadi panutan dan seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
11. Keluarga besar HIMASISKO yang telah membersamai dan membantu dalam hal perkuliahan selama ini.
12. Seluruh saudara dari pihak Ibu dan Ayah yang selalu mendoakan dan memberi dukungan kepada saya.
13. My Best Partner Dede Andreansyah yang selalu mendoakan dan memberi dukungan kepada saya.
14. Teman Kocakku Fitri, Diah, Ega, Icha, Mey, Octa, Aji yang selalu mendoakan dan memberi dukungan kepada saya.
15. Teman Princessku Nova, Cindo, Anti, Dwi Juny, Rany. Teman Bobrokku Winarti, Dhea, Mila, Nana yang selalu mendoakan dan memberi dukungan kepada saya.
16. Teman Comring Communityku Yuk Dewi, Yuk Pemi, Yuk Cica, Ona, Iput, Berli, Tri, Adi, Agung Pratama, Mona, Ara, Yuni, Agung, Ryan, Maya, Keke, Kiki, Novi, Sepa, Yuk Yona, Shifa yang selalu mendoakan dan memberi dukungan kepada saya.
17. Teman Ceriaku Della, Sandra, Lili yang selalu mendoakan dan memberi dukungan kepada saya.
18. Teman Kecilku, Yuk Ica, Dek Ipul, Dek Pani, Unus yang selalu mendoakan dan memberi dukungan kepada saya.
19. Teman SDku Semua Alumni kelas 6A dan 6B yang selalu mendoakan dan memberi dukungan kepada saya.

20. Teman SMPku Yati, Mira, Deffi Semua Kelas 91, 92, 93, 94 yang selalu mendoakan dan memberi dukungan kepada saya.
21. Teman SMAku Peri, Alen, Aji, Sesa, Semua Kelas IPA 1 dan IPA 2 yang selalu mendoakan dan memberi dukungan kepada saya.
22. Teman SK16 A yang selalu mendoakan dan memberi dukungan kepada saya.
23. Team Riset Comnet Deri, Ardin, Anut, Gioh, Adel, Hari Ahmad, Yogik, Aji, Arya, Ejak, Fakhri, Farhan, Octa, Toriq, Hakim yang selalu mendoakan dan memberi dukungan kepada saya.
24. Kak Bram, Kak Ade, Kak Azwar, Kak Novit, Kak Juanda, Kak Aldo, Kak Fahron, Kak Somame, Mba Resti yang selalu mendoakan dan memberi dukungan kepada saya.
25. Kucing-kucing tercinta Molly, Beki, Ganas, Miky, Millo, Mio, Momo, Sojun, Mimo.
26. Jurusan Sistem Komputer.
27. Almamater.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Tugas Akhir ini. Karena sesungguhnya tak ada yang sempurna didunia ini. Untuk itu, segala saran dan kritik sangatlah penting bagi penulis. Akhir kata, semoga Tugas Akhir ini dapat bermanfaat dan berguna bagi khalayak.

Indralaya, Juli 2021  
Penulis

Widyana Aprianti  
NIM. 09011181621010

**Implementasi *Principal Component Analysis* (PCA) Dan Algoritma *Naïve Bayes Classifier* Pada Klasifikasi Botnet Di Jaringan Internet Of Things (IoT)**

**Widyana Aprianti (0901118162110)**

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

Email : widyanaaprianti@gmail.com

**Abstrak**

*Botnet* merupakan sebuah program yang merusak sistem jaringan dan menyebar keseluruh komputer melalui internet. *Bot* melakukan tindakan seperti mengirim permintaan ke situs web target dengan maksud merubah situs menjadi serangan. Pada penelitian ini menggunakan dataset MedBIoT dengan tiga jenis *botnet* yaitu *mirai*, *torii*, dan *bashlite*. *Principal Component Analysis* (PCA) digunakan untuk mengurangi dimensi data dengan membuat variabel baru dalam jumlah yang lebih kecil. Algoritma *Naïve Baye Classifier* terdiri dari dua model yaitu Model *Bernoulli* dan *Gaussian*. Hasil dari penelitian ini membuktikan bahwa algoritma *Naïve Baye Classifier* menggunakan *Principal Component Analysis* (PCA) dapat melakukan proses klasifikasi botnet dengan baik. Hasil klasifikasi menggunakan model *Gaussian* sebagai hasil terbaik yaitu dengan nilai akurasi sebesar 97.71%, presisi sebesar 96.90%, dan recall sebesar 97.49%.

**Kata Kunci :** *Botnet Classification*, MedBIoT, *Principal Component Analysis* (PCA), *Naïve Bayes Classifier*

**Implementation of Principal Component Analysis (PCA) and Naive Bayes  
Classifier Algorithm for Botnet Classification in Internet Of Things (IoT)  
Networks**

**Widyana Aprianti (0901118162110)**

Department of Computer Engineering, Faculty of Computer Science

Universitas Sriwijaya

Email : widyanaaprianti@gmail.com

**Abstract**

A botnet is a program that destroys a network system and spreads to all computers via the internet. The bot performs actions such as sending a request to the target website by turning the site into an attack. In this study using the MedBIoT dataset with three types of botnets, namely mirai, torii, and bashlite. Principal Component Analysis (PCA) is used to reduce dimensional data by creating a small number of new variables. The Naïve Baye Classifier algorithm consists of two models, namely the Bernoulli and Gaussian models. The results of this study prove that the Naïve Baye Classifier algorithm using Principal Component Analysis (PCA) can perform the botnet classification process well. The results of the classification using the Gaussian model as the best result with an accuracy value of 97.71%, precision 96.90%, and recall 97.49%.

**Keywords :** Botnet Classification, MedBIoT, Principal Component Analysis (PCA), Naïve Baye Classifier

## DAFTAR ISI

	<b>Halaman</b>
<b>HALAMAN JUDUL .....</b>	<b>i</b>
<b>HALAMAN PENGESAHAN .....</b>	<b>ii</b>
<b>HALAMAN PERSETUJUAN .....</b>	<b>iii</b>
<b>HALAMAN PERNYATAAN .....</b>	<b>iv</b>
<b>HALAMAN PERSEMBAHAN .....</b>	<b>v</b>
<b>KATA PENGANTAR .....</b>	<b>vi</b>
<b>ABSTRAK .....</b>	<b>ix</b>
<b>ABSTRACT .....</b>	<b>x</b>
<b>DAFTAR ISI .....</b>	<b>xi</b>
<b>DAFTAR GAMBAR .....</b>	<b>xiv</b>
<b>DAFTAR TABEL .....</b>	<b>xv</b>
 <b>BAB I PENDAHULUAN</b>	
1.1 Latar Belakang .....	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan.....	3
1.5 Manfaat .....	3
1.6 Metodologi Penelitian .....	3
1.7 Sistematika Penulisan.....	4

## **BAB II TINJAUAN PUSTAKA**

2.1 Pendahuluan .....	6
2.2 Analisis <i>Malware</i> Statis .....	6
2.3 <i>Botnet</i> .....	6
2.3.1 Analisis <i>Botnet</i> .....	6
2.3.2 <i>Botnet Mirai</i> .....	7
2.4 Dataset.....	8
2.4.1 <i>Data Extraction</i> .....	9
2.4.2 <i>Principal Component Analysis (PCA)</i> .....	9
2.5 <i>Naïve Bayes Classifier</i> .....	9
2.5.1 <i>Naïve Bayes Classifier</i> Model <i>Bernoulli</i> .....	10
2.5.1 <i>Naïve Bayes Classifier</i> Model <i>Gaussian</i> .....	11
2.6 Evaluasi Performa .....	11

## **BAB III METODOLOGI**

3.1 Pendahuluan .....	13
3.2 Diagram Konsep Penelitian .....	13
3.3 Kerangka Kerja .....	14
3.4 Perancangan Sistem .....	16
3.4.1 Kebutuhan Perangkat Keras dan Perangkat Lunak.....	16
3.5 Dataset .....	17
3.5.1 <i>Data Extraction</i> .....	17
3.6 <i>Principal Component Analysis (PCA)</i> .....	20
3.7 Algoritma <i>Naïve Bayes Classifier</i> .....	22

3.8 Validasi .....	23
3.8.1 Validasi <i>Fine Tuning</i> Pada Skenario 1 .....	23
3.8.1 Validasi <i>Fine Tuning</i> Pada Skenario 2 .....	24
<b>BAB IV HASIL DAN ANALISA</b>	
4.1 Pendahuluan .....	26
4.2 Dataset.....	26
4.2.1 Tampilan Data Sebelum Dilakukan <i>Extraction</i> .....	26
4.2.2 Tampilan Data Sesudah Dilakukan <i>Extraction</i> .....	27
4.3 <i>Cleaning</i> Data.....	29
4.3.1 Tampilan Data Sebelum dilakukan <i>Cleaning</i> Data .....	29
4.3.2 Tampilan Data Sesudah dilakukan <i>Cleaning</i> Data .....	31
4.4 PCA .....	32
4.5 Perhitungan Hasil Validasi.....	33
4.5.1 Validasi <i>Fine Tuning</i> Pada Model <i>Bernoulli</i> .....	33
4.5.2 Validasi <i>Fine Tuning</i> Pada Model <i>Gaussian</i> .....	36
4.5.4 Analisa .....	39
<b>BAB V KESIMPULAN</b>	
5.1 Kesimpulan .....	41
5.2 Saran.....	42
<b>DAFTAR PUSTAKA .....</b>	43

## DAFTAR GAMBAR

<b>Gambar 2.1.</b> Alur Kerja <i>Botnet Mirai</i> Pada DDoS .....	8
<b>Gambar 3.1.</b> Diagram Konsep Penelitian .....	13
<b>Gambar 3.2.</b> Kerangka Kerja Penelitian.....	15
<b>Gambar 3.3.</b> Diagram Data <i>Extraction</i> .....	18
<b>Gambar 3.4.</b> <i>Flowchart Principal Component Analysis</i> .....	21
<b>Gambar 3.5.</b> <i>Flowchart Naïve Bayes Classifier</i> .....	22
<b>Gambar 4.1.</b> Data PCAP <i>Botnet Mirai</i> .....	26
<b>Gambar 4.2.</b> Data PCAP Normal.....	27
<b>Gambar 4.3.</b> Hasil Data <i>Extraction</i> Data <i>Botnet Mirai</i> .....	27
<b>Gambar 4.4.</b> Hasil Data <i>Extraction</i> Data Normal.....	28
<b>Gambar 4.5.</b> Hasil Penggabungan Data <i>Botnet Mirai</i> dan Normal .....	28
<b>Gambar 4.6.</b> Diagram Jumlah Data <i>Botnet Mirai</i> dan Data Normal .....	29
<b>Gambar 4.7.</b> Hasil Dataset Sebelum Dilakukan <i>Cleaning Data</i> .....	30
<b>Gambar 4.8.</b> Hasil Dataset Sesudah Dilakukan <i>Cleaning Data</i> .....	32
<b>Gambar 4.9.</b> <i>Scatterplot</i> Hasil <i>Principal Component Analysis</i> .....	33
<b>Gambar 4.10.</b> Hasil <i>Precision Recall Curve</i> Pada Model <i>Bernoulli</i> Perbandingan <i>Training</i> 70% dan <i>Testing</i> 30%.....	34
<b>Gambar 4.11.</b> <i>Scatterplot Naïve Bayes Classifier</i> Model <i>Bernoulli</i> .....	35
<b>Gambar 4.12.</b> Hasil <i>Precision Recall Curve</i> Pada Model <i>Gaussian</i> Perbandingan <i>Training</i> 70% dan <i>Testing</i> 30% .....	37
<b>Gambar 4.13.</b> <i>Scatterplot Naïve Bayes Model Gaussian</i> .....	38
<b>Gambar 4.14.</b> Grafik Perbandingan <i>Accuracy</i> Model <i>Bernoulli</i> dan <i>Gaussian</i> ...	40

## DAFTAR TABEL

<b>Tabel 1.</b> <i>Confusion Matrix</i> .....	11
<b>Tabel 2.</b> <i>Spesifikasi Perangkat Keras</i> .....	16
<b>Tabel 3.</b> <i>Spesifikasi Perangkat Lunak</i> .....	16
<b>Tabel 4.</b> Pembagian Kelas dan jumlah data .....	17
<b>Tabel 5.</b> Tampilan Dataset Hasil <i>Extraction</i> .....	19
<b>Tabel 6.</b> Validasi Skenario 1 .....	23
<b>Tabel 7.</b> Validasi Skenario 2 .....	25
<b>Tabel 8.</b> Fitur Sebelum Dilakukan <i>Cleaning Data</i> .....	30
<b>Tabel 9.</b> Fitur Sesudah Dilakukan <i>Cleaning Data</i> .....	31
<b>Tabel 10.</b> Hasil <i>Reduced Data</i> .....	32
<b>Tabel 11.</b> Hasil Validasi Model <i>Bernoulli</i> Pada Performa <i>Confusion Matrix</i> .....	34
<b>Tabel 12.</b> Hasil <i>Confusion Matrix</i> Model <i>Bernoulli</i> .....	35
<b>Tabel 11.</b> Hasil Validasi Model <i>Gaussian</i> Pada Performa <i>Confusion Matrix</i> .....	37
<b>Tabel 12.</b> Hasil <i>Confusion Matrix</i> Model <i>Gaussian</i> .....	38



## **BAB 1**

### **PENDAHULUAN**

#### **1.1 Latar Belakang**

*Botnet* merupakan sebuah program yang merusak sistem jaringan dan menyebar keseluruh komputer melalui internet. *Botnet* terdiri dari komputer yang sudah terinfeksi dan dapat dikendalikan dari jarak jauh oleh penyerang. *Bot* menghubungi server jarak jauh pada waktu tertentu, sehingga dapat menginstruksi penyerang dalam melakukan tindakan. *Bot* melakukan tindakan seperti mengirim permintaan ke situs web target dengan maksud merubah situs menjadi serangan [1]. Seorang "Botmaster" akan menguasai jaringan komputer yang terinfeksi melalui sistem C&C. *Botnet* berbasis IoT dalam kasus ini adalah *Botnet Mirai*. Serangan dilakukan menggunakan *Botnet Mirai*, sehingga dapat melacak IoT untuk membuat program serangan lainnya pada sebuah perangkat [2]. *Mirai* melakukan pemindahan akses secara luas dari *IP address* untuk menemukan perangkat IoT, yang dapat diakses melalui *login credentials* sehingga mudah diketahui.

*Principal Component Analysis* (PCA) digunakan untuk mengurangi dimensi data dengan membuat variabel baru dalam jumlah yang lebih kecil. PCA merupakan metode linier dari proses ekstraksi fitur yang paling umum digunakan [3]. PCA digunakan untuk mengekstrak informasi dari kumpulan data, kemudian ditampilkan sebagai satu set variable *orthogonal* baru yang disebut komponen utama. PCA dapat digunakan untuk menghasilkan akurasi yang tinggi dan mampu mencapai perhitungan menggunakan komputer yang cukup efisien. PCA digunakan untuk mereduksi dimensi tanpa merubah parameter-parameter penting dalam data tersebut.

Pada penelitian ini menggunakan metode *Naïve Bayes Classifier* yang merupakan sebuah jenis probabilitas Bayesian yang sederhana [4]. Pada pendekatan *naïve bayes* [5] semua atribut yang dimiliki tidak saling berhubungan, ini juga yang membuat prediksi lebih akurat dan lebih cepat.

Pada penelitian [6] melakukan analisis eksperimental metode pada *machine learning* untuk mendeteksi serangan botnet DDoS menggunakan data NB 15 dengan nilai akurasi pada *naïve bayes* 71.63%. Selanjutnya, dalam penelitian [7] menggunakan pendekatan *lightweight* untuk mendeteksi *malware* DDoS pada IoT. Peneliti mengekstrak sebuah gambar malware menggunakan *lightweight convolutional neural network*. Hasil akurasi yang didapat mencapai 94.0% untuk klasifikasi *goodware* dan *malware* DDoS dan akurasi 81.8% untuk klasifikasi *goodware* dan dua kelompok *malware* utama. Kemudian, metode *Naïve Bayes* digunakan untuk mendeteksi berita palsu [8]. Pendekripsi yang diimplementasikan pada postingan berita yang ada di *facebook* dengan nilai akurasi 74%.

Berdasarkan penjelasan diatas, peneliti akan melakukan cara mengimplementasi sistem pengklasifikasi *botnet* di jaringan IoT dengan judul “Implementasi *Principal Component Analysis* (PCA) dan Algoritma *Naïve Bayes Classifier* Pada Klasifikasi *Botnet* di Jaringan Internet of Things (IoT)”.

## 1.2 Perumusan Masalah

Berikut adalah rumusan masalah dalam penulisan Proposal Tugas Akhir ini:

1. Bagaimana cara mereduksi dataset menggunakan *Principal Component Analysis* (PCA)?
2. Bagaimana cara mengklasifikasi serangan *Botnet* menggunakan Algoritma *Naïve Bayes Classifier*?
3. Apa saja *output* yang dihasilkan dari algoritma *Naïve Bayes Classifier* pada serangan *Botnet*?

## 1.3 Batasan Masalah

Berikut adalah ruang lingkup masalah dalam penulisan Proposal Tugas Akhir ini:

1. Dataset yang digunakan adalah dataset MedBIoT [9].
2. Mengklasifikasi serangan *Botnet* pada jaringan *Internet of Things* (IoT) Menggunakan Algoritma *Naïve Bayes Classifier*.
3. Serangan *Botnet* yang dibahas adalah *Malware Mirai*.

4. Proses *Dimensionality Reduction* menggunakan *Principal Component Analysis* (PCA).
5. Tidak membahas megenai pencegahan

#### **1.4 Tujuan**

Adapun tujuan dari penulisan Proposal Tugas Akhir ini adalah sebagai berikut :

1. Melakukan *Dimensionality Rduction* menggunakan *Principal Component Analysis* (PCA).
2. Mengklasifikasi Botnet menggunakan algoritma *naïve bayes classifier*.
3. Mendapatkan output yang dihasilkan dari algoritma *Naïve Bayes Classifier* pada serangan *Botnet*.

#### **1.5 Manfaat**

Adapun manfaat dari penulisan Proposal Tugas Akhir ini adalah sebagai berikut :

1. Dapat melakukan *Dimensionality Reduction* menggunakan *Principal Component Analysis* (PCA).
2. Dapat mengimplementasikan Algoritma *Naïve Bayes Classifier* pada pengklasifikasian di jaringan *Internet of Things* (IoT).
3. Dapat menghasilkan output dari algoritma *Naïve Bayes Classifier* pada serangan *Botnet*.

#### **1.6 Metodologi Penelitian**

Metodologi yang digunakan dalam penulisan tugas akhir ini akan melewati beberapa tahapan sebagai berikut :

1. Tahap Pertama (Studi Pustaka/literature)

Dalam tahap ini dilakukan setelah masalah yang akan dibahas sudah sesuai dengan mencari informasi yang diperlukan melalui media pembelajaran seperti jurnal ilmiah, buku, internet, serta artikel-artikel terkait yang mendukung penulisan Proposal Tugas Akhir ini.

## 2. Tahap Kedua (Perancangan Sistem)

Pada tahap ini dilakukan penerapan metode pada sistem penelitian. Kemudian, pada tahapan ini juga membangun dan menerapkan metode yang akan digunakan serta menyiapkan *hardware* dan *software* serta melakukan kofigurasi ataupun menulis *code* untuk penerapan metode ada tugas akhir.

## 3. Tahap Ketiga (Pengujian)

Dalam tahap ini, peneliti melakukan tahapan pengujian metodologi penelitian dan penelitian sebelumnya sehingga didapatkan data hasil uji yang sesuai dan tepat dengan algoritma.

## 4. Tahap Keempat (Analisa)

Tahap ini merupakan tahapan menganalisa data hasil pengujian dengan diterapkan pendekatan tertentu, sehingga didapat hasil yang objektif dimana data diperoleh dari pengujian.

## 5. Tahap Kelima (Kesimpulan dan Saran)

Pada tahap ini akan dilakukan kesimpulan berdasarkan permasalahan, studi pustaka, metodologi penelitian, dan analisa hasil pengujian. Serta saran untuk penulis selanjutnya jika ingin dijadikan referensi.

## 1.7 Sistematika Penulisan

Adapun sistematika penulisan dalam Proposal Tugas Akhir ini adalah sebagai berikut:

### 1. BAB I. PENDAHULUAN

Pada bab I akan berisikan latar belakang masalah, tujuan dan manfaat serta metodologi penelitian dan sistemaika penulisan.

### 2. BAB II. TINJAUAN PUSTAKA

Pada Bab II akan berisi dasar teori *Malware*, *Botnet*, *Dataset*, *Principal Component Analysis* (PCA) dan *Naïve Bayes Classifier*.

### **3. BAB III. ANALISIS DAN PERANCANGAN**

Pada Bab III akan membahas analisis dan perancangan sistem klasifikasi serangan *Botnet Mirai* menggunakan *Principal Component Analysis* (PCA) dan *Naïve Bayes Classifier*.

### **4. BAB IV. IMPLEMENTASI PENGUJIAN**

Pada Bab IV akan membahas hasil pengklasifikasian *Botnet Mirai* yang diperoleh menggunakan *Principal Component Analysis* (PCA) dan *Naïve Bayes Classifier* serta melakukan validasi hasil.

### **5. BAB V. KESIMPULAN**

Pada bab V berisi kesimpulan dari bab-bab yang sudah dicantumkan mengenai hasil. Pada bab ini juga akan berisi jawaban-jawaban dari tujuan yang sudah dibuat.

## DAFTAR PUSTAKA

- [1] E. Bertino, “Botnets and Internet,” *Computer (Long. Beach. Calif.)*, pp. 76–79, 2017, doi: 10.1109/MC.2017.62.
- [2] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-mariona, “IoDDoS — The Internet of Distributed Denial of Service Attacks A Case Study of the Mirai Malware and IoT-Based Botnets,” no. IoTBDS, pp. 978–989, 2017, doi: 10.5220/0006246600470058.
- [3] D. H. Hoang and H. D. Nguyen, “A PCA-based method for IoT network traffic anomaly detection,” *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2018-Febru, pp. 381–386, 2018, doi: 10.23919/ICACT.2018.8323766.
- [4] S. Mukherjee and N. Sharma, “Intrusion Detection using Naive Bayes Classifier with Feature Reduction,” *Procedia Technol.*, vol. 4, pp. 119–128, 2012, doi: 10.1016/j.protcy.2012.05.017.
- [5] N. A. Singh, J. Singh, and T. De, “Distributed denial of service attack detection using naive bayes classifier through info gain feature selection,” *ACM Int. Conf. Proceeding Ser.*, vol. 25-26-Augu, 2016, doi: 10.1145/2980258.2980379.
- [6] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, and N. T. K. Son, “Performance evaluation of Botnet DDoS attack detection using machine learning,” *Evol. Intell.*, vol. 13, no. 2, pp. 283–294, 2020, doi: 10.1007/s12065-019-00310-w.
- [7] J. Su, V. Danilo Vasconcellos, S. Prasad, S. Daniele, Y. Feng, and K. Sakurai, “Lightweight Classification of IoT Malware Based on Image Recognition,” *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 2, pp. 664–669, 2018, doi: 10.1109/COMPSAC.2018.10315.
- [8] C. Troussas, M. Virvou, K. J. Espinosa, K. Llaguno, and J. Caro, “Sentiment analysis of Facebook statuses using Naive Bayes Classifier for

- language learning,” *IISA 2013 - 4th Int. Conf. Information, Intell. Syst. Appl.*, pp. 198–205, 2013, doi: 10.1109/IISA.2013.6623713.
- [9] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, and S. Nõmm, “MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network,” *ICISSP 2020 - Proc. 6th Int. Conf. Inf. Syst. Secur. Priv.*, no. Icissp, pp. 207–218, 2020, doi: 10.5220/0009187802070218.
- [10] A. P. Namanya, A. Cullen, I. U. Awan, and J. P. Disso, “The World of Malware: An Overview,” *Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud, FiCloud 2018*, pp. 420–427, 2018, doi: 10.1109/FiCloud.2018.00067.
- [11] R. Islam, R. Tian, L. M. Batten, and S. Versteeg, “Classification of malware based on integrated static and dynamic features,” *J. Netw. Comput. Appl.*, vol. 36, no. 2, pp. 646–656, 2013, doi: 10.1016/j.jnca.2012.10.004.
- [12] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas, “DDoS in the IoT: Mirai and Other Botnets,” *Computer (Long Beach. Calif.)*, p. 1, 2017.
- [13] M. Antonakakis *et al.*, “Understanding the Mirai Botnet This paper is included in the Proceedings of the Understanding the Mirai Botnet,” *USENIX Secur.*, pp. 1093–1110, 2017, [Online]. Available: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis>.
- [14] . S. S., “Improved Spambase Dataset Prediction Using Svm Rbf Kernel With Adaptive Boost,” *Int. J. Res. Eng. Technol.*, vol. 04, no. 06, pp. 383–386, 2015, doi: 10.15623/ijret.2015.0406064.
- [15] M. Morchid, R. Dufour, P. M. Bousquet, G. Linarès, and J. M. Torres-Moreno, “Feature selection using Principal Component Analysis for massive retweet detection,” *Pattern Recognit. Lett.*, vol. 49, pp. 33–39, 2014, doi: 10.1016/j.patrec.2014.05.020.

- [16] A. Burrello, A. Marchioni, D. Brunelli, and L. Benini, “Embedding Principal Component Analysis for Data Reduction in Structural Health Monitoring on Low-Cost IoT Gateways,” *ACM Int. Conf. Comput. Front. 2019, CF 2019 - Proc.*, pp. 235–239, 2019, doi: 10.1145/3310273.3322822.
- [17] Y. Ye, D. Wang, T. Li, D. Ye, and Q. Jiang, “An intelligent PE-malware detection system based on association mining,” *J. Comput. Virol.*, vol. 4, no. 4, pp. 323–334, 2008, doi: 10.1007/s11416-008-0082-4.
- [18] Institute of Electrical and Electronics Engineers. Ukraine Section, Institute of Electrical and Electronics Engineers. Region 8, European Microwave Association, and Institute of Electrical and Electronics Engineers, “2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON) : conference proceedings : May 29-June 2, 2017, Kyiv, Ukraine,” pp. 900–903, 2017.
- [19] X. Deng, Q. Liu, Y. Deng, and S. Mahadevan, “An improved method to construct basic probability assignment based on the confusion matrix for classification problem,” *Inf. Sci. (Ny).*, vol. 340–341, pp. 250–261, 2016, doi: 10.1016/j.ins.2016.01.033.