

**PENERAPAN *ML-BASED INTRUSION DETECTION SYSTEM*  
UNTUK DETEKSI SERANGAN TERHADAP KEAMANAN  
JARINGAN DI LINGKUNGAN ISB ATMA LUHUR**

**SKRIPSI**



Irfan Yahya  
1911500083

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
INSTITUT SAINS DAN BISNIS ATMA LUHUR  
PANGKALPINANG  
2023**

**PENERAPAN *ML-BASED INTRUSION DETECTION SYSTEM*  
UNTUK DETEKSI SERANGAN TERHADAP KEAMANAN  
JARINGAN DI LINGKUNGAN ISB ATMA LUHUR**

**SKRIPSI**

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



Oleh:

Irfan Yahya  
1911500083

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
INSTITUT SAINS DAN BISNIS ATMA LUHUR  
PANGKALPINANG  
2023**

## LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

NIM : 1911500083

Nama : Irfan Yahya

Judul Skripsi : PENERAPAN *ML-BASED INTRUSION DETECTION SYSTEM* UNTUK DETEKSI SERANGAN TERHADAP KEAMANAN JARINGAN DI LINGKUNGAN ISB ATMA LUHUR

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 04 Agustus 2023

A 1000 Rupiah postage stamp with a signature over it. The stamp features the Garuda Pancasila emblem and the text '1000', 'METERAL TEMPEL', and '6A6AKX542620281'. The signature is written in black ink over the stamp.

(Irfan Yahya)

**LEMBAR PENGESAHAN SKRIPSI**

**PENERAPAN ML-BASED INTRUSION DETECTION SYSTEM UNTUK  
DETEKSI SERANGAN TERHADAP KEAMANAN JARINGAN DI  
LINGKUNGAN ISB ATMA LUHUR**

Yang dipersiapkan dan disusun oleh

**Irfan Yahya**

**1911500083**

Telah dipertahankan di depan Dewan Penguji

Pada tanggal, 07 Agustus 2023

**Anggota Penguji**



**Devi Irawan, M.Kom**  
NIDN. 0231018201

**Dosen Pembimbing**



**Harrizki Arie P, S.Kom., M. T.**  
NIDN. 0213048601

**Kaprodi Teknik Informatika**



**Chandra Kirana, M.Kom**  
NIDN. 0228108501

**Ketua Penguji**



**Yurindra, S.Kom., M. T.**  
NIDN. 0429057402

Skripsi ini telah diterima dan sebagai salah satu persyaratan


Untuk memperoleh gelar Sarjana Komputer

Tanggal 07 Agustus 2023

**DEKAN FAKULTAS TEKNOLOGI INFORMASI**

**ISB ATMA LUHUR**



  
**Ellya Hel mud, M.Kom**  
NIDN. 0201027901

## KATA PENGANTAR

Puji syukur kita panjatkan kepada Allah SWT atas segala rahmat dan karunia-Nya yang telah diberikan berupa kemampuan, kesehatan dan juga kesempatan, sehingga penulis dapat menyelesaikan skripsi yang berjudul “**PENERAPAN ML-BASED INTRUSION DETECTION SYSTEM UNTUK MENDETEKSI SERANGAN TERHADAP KEAMANAN JARINGAN DI LINGKUNGAN ISB ATMA LUHUR**” sebagai salah satu syarat untuk memperoleh gelar sarjana komputer.

Dalam penyusunan dan penulisan proposal skripsi ini penulis menyadari bahwa proposal ini tidak akan terwujud tanpa izin, bantuan, dan bimbingan dari berbagai pihak baik moral maupun materi. Oleh karena itu penulis mengucapkan terima kasih kepada :

1. Allah SWT yang telah memberikan kekuatan, kemampuan, kesehatan, kesabaran dan ketekunan untuk menyelesaikan laporan skripsi ini.
2. Bapak dan Ibu juga keluarga penulis yang tercinta, yang selalu memberikan dukungan baik moral, materi, doa, semangat dan kasih sayang.
3. Bapak Drs. Djaetun Hs selaku pendiri ISB Atma Luhur Pangkalpinang.
4. Bapak Drs. Harry Sudjianto, M.M., M.B.A. Selaku Ketua Pengurus Yayasan Atma Luhur Pangkalpinang
5. Bapak Prof. Dr. Moedjiono, M.Sc, selaku Rektor Institut Sains dan Bisnis (ISB) Atma Luhur Pangkalpinang.
6. Bapak Harrizki Arie Pradana, S.Kom., M.T. selaku Wakil Rektor 3 serta dosen pembimbing skripsi yang telah memberikan arahan, bimbingan, serta saran dalam penyusunan laporan skripsi ini.
7. Bapak Ellya Helmud, M.Kom, selaku Dekan Institut Sains dan Bisnis (Atma Luhur Pngkalpinang).
8. Bapak Chandra Kirana, M.Kom, selaku Ketua Program Studi Teknik Informatika (TI) Institut Sains dan Bisnis Atma Luhur Pangkalpinang.
9. Bapak Yohanes Setiawan Japriadi, S.Kom, M.Kom. selaku Direktur Biro Sistem Informasi Institut Sains dan Bisnis Atma Luhur Pangkalpinang

10. Sahabat dan seluruh teman-teman seperjuangan angkatan 2019 yang telah memberikan dukungan dalam menyelesaikan penyusunan proposal skripsi ini.

Penulis juga meminta maaf jika dalam penulisan laporan skripsi ini masih terdapat kesalahan baik dari kata, penulisan, maupun pemahaman dan penulis sangat mengharapkan kritik dan saran dari pihak-pihak yang membaca laporan ini. Akhir kata semoga laporan skripsi ini dapat berguna dan memberikan manfaat dalam menambah wawasan keilmuan.

Pangkalpinang, 31 Juli 2023

(Irfan Yahya)



## **ABSTRACT**

*Interest and advancements in internet and communication technology have made network security a highly significant research field. To ensure the security of networks and all connected assets in cyberspace, tools such as firewalls, antivirus software, and intrusion detection systems (IDS) are implemented. This research aims to design a machine learning-based intrusion detection system model using the decision tree algorithm. In the past decade, the development and utilization of machine learning have played a significant role in the advancement of IDS (Intrusion Detection System) and cybersecurity in general. In machine learning, models can learn from data and identify new patterns that indicate attacks, thereby detecting previously unseen attacks. The primary goal of implementing machine learning in cybersecurity is to make intrusion detection processes more actionable, measurable, and effective compared to traditional approaches, which require human intervention. The results of this research include a machine learning model capable of classifying normal network traffic and malicious network traffic. The performance results of the ML-Based IDS model tested show an overall classification accuracy of 93% on the provided sample data.*

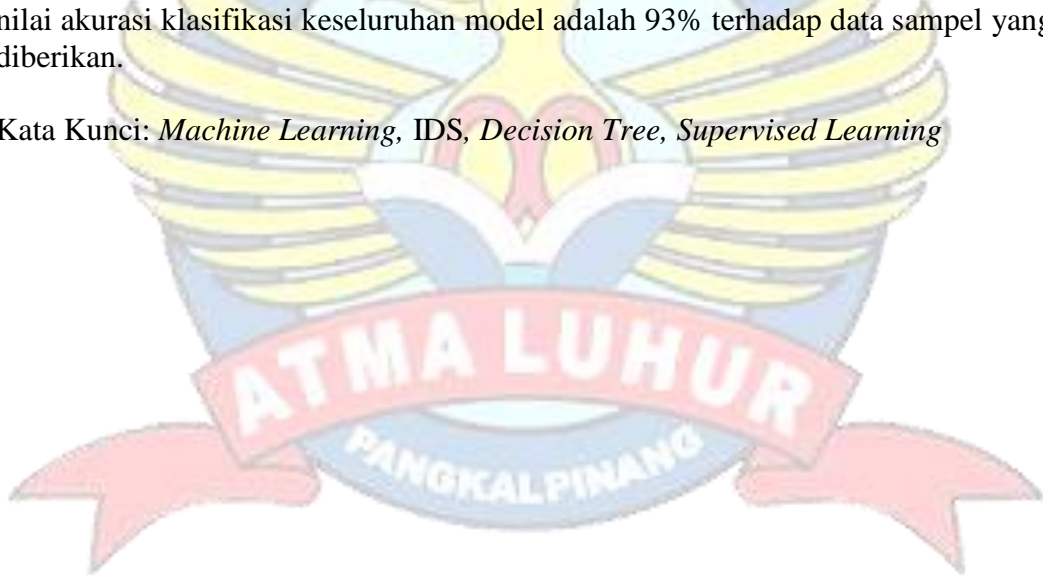
*Keywords: Machine Learning, IDS, Decision Tree, Supervised Learning.*



## ABSTRAK

Minat dan perkembangan dalam teknologi internet dan komunikasi telah menyebabkan keamanan jaringan menjadi bidang penelitian yang sangat penting. Untuk memastikan keamanan jaringan dan semua aset yang terhubung dalam ruang siber, diimplementasikan alat-alat seperti *firewall*, *antivirus*, dan sistem pendeteksi intrusi atau IDS. Penelitian ini bertujuan untuk merancang sebuah model *machine learning-based intrusion detection system* menggunakan algoritma *decision tree*. Pada dekade terakhir perkembangan dan penggunaan *machine learning* ikut ambil dalam perkembangan IDS (*intrusion detection system*) dan *cybersecurity* pada umumnya. Dalam *machine learning*, model dapat belajar dari data dan mencari pola baru yang menandakan serangan, sehingga dapat mendeteksi serangan yang belum pernah terjadi sebelumnya. Tujuan utama menerapkan *machine learning* dalam *cybersecurity* adalah untuk membuat proses deteksi intrusi lebih bisa ditindaklanjuti, terukur dan efektif daripada pendekatan tradisional, yang membutuhkan campur tangan manusia. Hasil penelitian ini berupa *machine learning model* yang mampu mengklasifikasi lalu lintas jaringan normal dan lalu lintas jaringan berbahaya. Hasil performa model ML-Based IDS yang diuji ialah nilai akurasi klasifikasi keseluruhan model adalah 93% terhadap data sampel yang diberikan.

Kata Kunci: *Machine Learning, IDS, Decision Tree, Supervised Learning*





## DAFTAR ISI

LEMBAR PERNYATAAN .....	i
LEMBAR PENGESAHAN .....	ii
KATA PENGANTAR .....	iii
<i>ABSTRACT</i> .....	v
ABSTRAK .....	vi
DAFTAR ISI .....	vii
DAFTAR GAMBAR .....	xi
DAFTAR TABEL .....	xiii
DAFTAR SIMBOL .....	xiv
DAFTAR LAMPIRAN .....	xviii
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah .....	3
1.4 Tujuan dan Manfaat Penelitian .....	3
1.4.1 Tujuan Penelitian .....	3
1.4.2 Manfaat Penelitian .....	4
1.5 Sistematika Penulisan .....	4
BAB II LANDASAN TEORI .....	6
2.1 UML ( <i>Unified Modeling Language</i> ) .....	6
2.1.1 <i>Use Case Diagram</i> .....	6
2.1.2 <i>Activity Diagram</i> .....	7
2.1.3 <i>Component Diagram</i> .....	7

2.1.4	<i>Deployment Diagram</i> .....	8
2.2	Keamanan Jaringan Komputer.....	8
2.3	Serangan Siber .....	9
2.4	IDS ( <i>Intrusion Detection System</i> ).....	9
2.4.1	<i>Host-Intrusion Detection System (HIDS)</i> .....	10
2.4.2	<i>Network Intrusion Detection System (NIDS)</i> .....	10
2.5	Jenis-jenis deteksi pada sistem IDS .....	11
2.5.1	Deteksi <i>Signature-Based</i> .....	11
2.5.2	Deteksi <i>Anomaly-Based</i> .....	11
2.5.3	Deteksi <i>ML-Based</i> .....	11
2.6	<i>Machine Learning</i> .....	12
2.6.1	Proses Pembelajaran pada <i>Machine Learning</i> .....	12
2.6.2	Jenis Pembelajaran pada <i>Machine Learning</i> .....	13
2.7	Algoritma <i>Decision Tree</i> .....	14
2.8	<i>Google Colab</i> .....	15
2.9	<i>Dataset NSL-KDD</i> .....	16
2.10	Tinjauan Penelitian Terdahulu .....	17
<b>BAB III METODOLOGI PENELITIAN</b> .....		<b>23</b>
3.1	Model Penelitian.....	23
3.2	Teknik Pengumpulan Data .....	25
3.2.1	Data Primer.....	25
3.2.2	Data Sekunder .....	25
3.3	Alat Bantu Pengembangan Sistem .....	26
3.3.1	UML .....	26
3.3.2	<i>Google Colab</i> .....	26

3.3.3	<i>Wireshark</i> .....	27
3.4	Algoritma Pendukung.....	27
3.4.1	Algoritma <i>Decision Tree</i> .....	27
BAB IV HASIL DAN PEMBAHASAN .....		28
4.1	Profil ISB Atma Luhur.....	28
4.1.1	Visi ISB Atma Luhur .....	28
4.1.2	Misi ISB Atma Luhur .....	29
4.1.3	Struktur Organisasi ISB Atma Luhur .....	29
4.2	Analisa Masalah.....	30
4.3	<i>Use Case Diagram</i> Penelitian.....	30
4.3.1	Deskripsi <i>Use Case Import Dataset</i> .....	31
4.3.2	Deskripsi <i>Use Case Data Pre-processing</i> .....	31
4.3.3	Deskripsi <i>Use Case Build ML Model</i> .....	32
4.3.4	Deskripsi <i>Use Case Training ML Model</i> .....	32
4.3.5	Deskripsi <i>Use Case Testing ML Model</i> .....	32
4.3.6	Deskripsi <i>Use Case Evaluasi ML Model</i> .....	32
4.4	<i>Activity Diagram</i> .....	33
4.4.1	<i>Activity Diagram Packet Capture</i> Trafik pada Jaringan <i>wifi.id</i> .....	33
4.4.2	<i>Activity Diagram</i> Penelitian <i>ML-Based Intrusion Detection System</i> .....	34
4.5	<i>Component Diagram</i> Penelitian.....	35
4.6	<i>Deployment Diagram</i> Penelitian.....	36
4.7	<i>Data Collection</i> .....	37
4.7.1	NSL-KDD .....	37
4.7.2	Data Hasil <i>Log Capture</i> di Jaringan <i>wifi.id</i> Kampus ISB Atma Luhur ..	38
4.8	Membangun Model <i>ML-Based IDS</i> pada <i>Google Colab Environment</i> ..	45

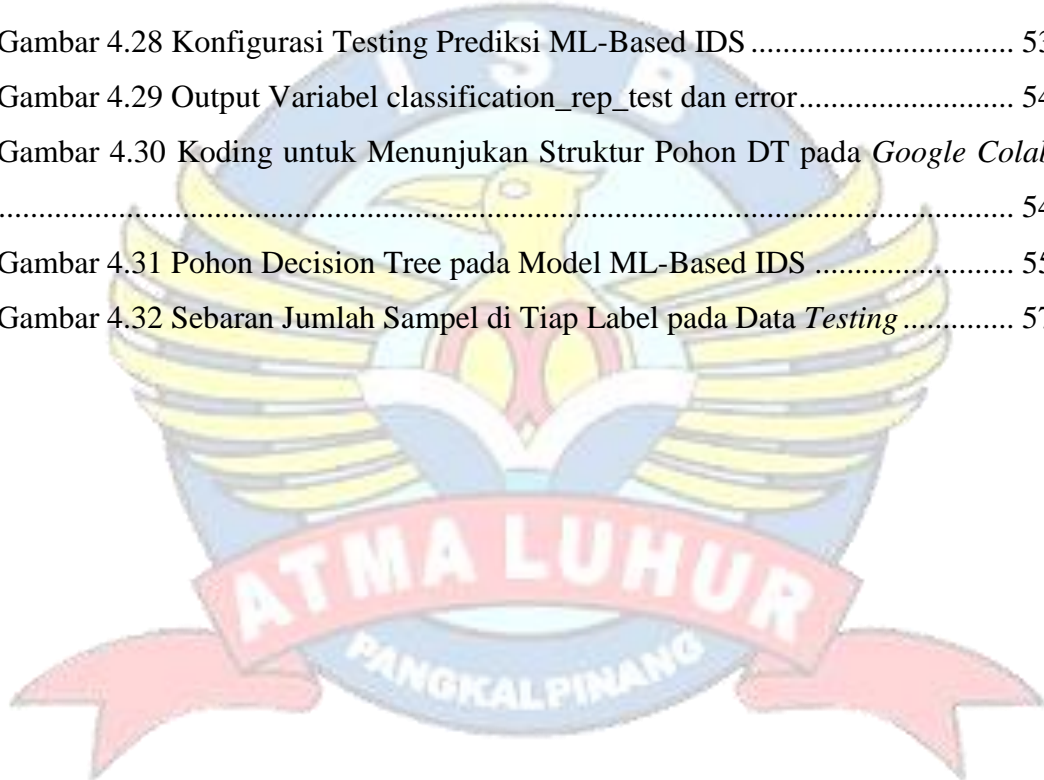
4.8.1	Konfigurasi awal dan <i>Import Library</i> yang Diperlukan .....	46
4.8.2	<i>Import Dataset</i> .....	46
4.8.3	Pemberian Nama Fitur dan Label pada Dataset.....	47
4.8.4	Data <i>Pre-processing</i> .....	49
4.8.5	<i>Training Phase</i> .....	51
4.8.6	<i>Testing Phase</i> dan Evaluasi Performa <i>ML-Based IDS</i> .....	53
BAB V PENUTUP.....		58
5.1	Kesimpulan .....	58
5.2	Saran .....	58
DAFTAR PUSTAKA .....		59
LAMPIRAN.....		62



## DAFTAR GAMBAR

Gambar 2.1 Contoh <i>Use Case Diagram</i> .....	6
Gambar 2.2 Contoh <i>Activity Diagram</i> .....	7
Gambar 2.3 Contoh <i>Component Diagram</i> .....	7
Gambar 2.4 Contoh <i>Deployment Diagram</i> .....	8
Gambar 2.5 Pohon Decision Tree .....	14
Gambar 3.1 Metode Pengembangan <i>Machine Learning Based IDS</i> .....	23
Gambar 4.1 Struktur Organisasi ISB Atma Luhur.....	29
Gambar 4. 2 <i>Use Case Diagram</i> Pengembangan <i>ML-Based IDS</i> .....	31
Gambar 4.3 <i>Activity Diagram Packet Capture</i> di Jaringan <i>wifi.id</i> Menggunakan Wireshark .....	33
Gambar 4.4 <i>Act4ity Diagram</i> Pengembangan <i>ML-Based IDS</i> .....	34
Gambar 4.5 <i>Deployment Diagram</i> Pengembangan <i>ML-Based IDS</i> .....	36
Gambar 4.6 5 data <i>head NSL-KDD Train+</i> .....	38
Gambar 4.7 Gedung 2 ISB Atma Luhur Pangkalpinang.....	38
Gambar 4.8 <i>Access Point wifi.id</i> Perpustakaan.....	39
Gambar 4. 9 <i>Packet Capture</i> Menggunakan <i>Wireshark</i> pada <i>wifi.id</i> perpustakaan ISB Atma Luhur.....	40
Gambar 4.10 Kantor Ruang Dekan.....	41
Gambar 4.11 <i>Access Point wifi.id</i> Kantor Dekan.....	41
Gambar 4.12 <i>Packet Capture</i> Menggunakan <i>Wireshark</i> pada <i>wifi.id</i> kantor Dekan ISB Atma Luhur.....	42
Gambar 4.13 Gedung 1 ISB Atma Luhur .....	43
Gambar 4.14 <i>Access Point wifi.id</i> Lantai 2 Gedung 1 ISB Atma Luhur .....	43
Gambar 4.15 <i>Packet Capture</i> Menggunakan <i>Wireshark</i> pada <i>wifi.id</i> Gedung 1 Atma Luhur .....	44
Gambar 4. 16 Data Capture Wireshark pada jaringan <i>wifi.id</i> ISB Atma Luhur ...	45
Gambar 4. 17 <i>Google Colab Environment</i> .....	45
Gambar 4.18 <i>Import Library</i> pada <i>Google Colab Environment</i> .....	46
Gambar 4.19 Konfigurasi Awal pada <i>Google Colab</i> .....	46

Gambar 4.20 <i>Import</i> Data Latih dan Data <i>Test</i> pada <i>Google Colab</i> .....	46
Gambar 4.21 <i>Array List</i> Nama Kolom untuk Fitur dan Label pada Dataset .....	47
Gambar 4.22 Pemisahan Tipe Data pada Kolom Fitur .....	49
Gambar 4.23 Pengaturan Kategori dan Tipe label Serangan .....	50
Gambar 4.24 Sebaran tipe serangan pada <i>dataset</i> pelatihan NSL-KDD .....	51
Gambar 4.25 Sebaran Kategori Serangan Dataset Pelatihan NSL-KDD.....	52
Gambar 4.26 <i>Assign Variabel</i> pada kurva X dan Y terhadap <i>dataset</i> .....	52
Gambar 4.27 Koding Bangun dan Latih ML-Based IDS menggunakan klasifikasi DT .....	53
Gambar 4.28 Konfigurasi Testing Prediksi ML-Based IDS .....	53
Gambar 4.29 Output Variabel <i>classification_rep_test</i> dan <i>error</i> .....	54
Gambar 4.30 Koding untuk Menunjukkan Struktur Pohon DT pada <i>Google Colab</i> .....	54
Gambar 4.31 Pohon Decision Tree pada Model ML-Based IDS .....	55
Gambar 4.32 Sebaran Jumlah Sampel di Tiap Label pada Data <i>Testing</i> .....	57



## DAFTAR TABEL

Tabel 2.1 Tinjauan Penelitian Terdahulu .....	17
Tabel 4.1 Deskripsi <i>Use Case Import Data Set</i> .....	31
Tabel 4.2 Deskripsi <i>Use Case Data Pre-processing</i> .....	31
Tabel 4.3 Deskripsi <i>Use Case Build ML Model</i> .....	32
Tabel 4.4 Deskripsi <i>Use Case Training ML Model</i> .....	32
Tabel 4.5 Deskripsi <i>Use Case Testing ML Model</i> .....	32
Tabel 4.6 Deskripsi <i>Use Case Evaluasi ML Model</i> .....	32
Tabel 4.7 Tipe dan Kategori Serangan Dataset NSL-KDD .....	50






## DAFTAR SIMBOL




### 1. Use Case Diagram



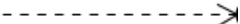

No	Gambar	Nama	Keterangan
1		<i>Actor</i>	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan <i>use case</i>
2		<i>Use Case</i>	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu <i>actor</i>
3		<i>Note</i>	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputansi
4		<i>Sistem</i>	Menspesifikasikan paket yang menampilkan sistem secara terbatas
5		<i>Include</i>	Menspesifikasikan bahwa <i>use case</i> sumber secara eksplisit
6		<i>Dependency</i>	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri ( <i>independent</i> ) akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri
7		<i>Generalization</i>	Hubungan dimana objek anak ( <i>decendent</i> ) berbagi perilaku dan



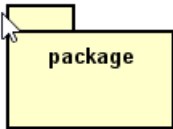
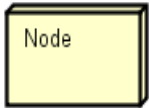

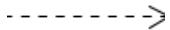
			struktur data dari objek yang ada di atasnya objek induk ( <i>ancestor</i> )
8		<i>Extend</i>	Menspesifikasikan bahwa <i>use case</i> target memperluas perilaku dari <i>use case</i> sumber pada suatu titik yang diberikan
9		<i>Association</i>	Apa yang menghubungkan antara objek satu dengan objek lainnya.
10		<i>Collaboration</i>	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan perilaku yang lebih besar dari jumlah dan elemen-elemennya

## 2. Activity Diagram

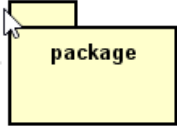



No	Gambar	Nama	Keterangan
1		<i>Nary Association</i>	Upaya untuk menghindari asosiasi dengan lebih dari 2 objek
2		<i>Generalization</i>	Hubungan dimana objek anak ( <i>decendent</i> ) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk ( <i>ancestor</i> )
3		<i>Collaboration</i>	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu <i>actor</i>

4		<i>Class</i>	Himpunan dari objek-objek yang berbagi atribut serta operasi yang sama
5		<i>Realization</i>	Operasi yang benar-benar dilakukan oleh suatu objek
6		<i>Dependency</i>	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri ( <i>independent</i> ) akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri
7		<i>Association</i>	Apa yang menghubungkan antara objek satu dengan objek lainnya

### 3. Deployment Diagram

No	Gambar	Nama	Keterangan
1		Package	Untuk mengelompokkan satu atau lebih node
2		Node	Biasanya mengacu pada hardware dan software
3		Link	Relasi antara node
4		Dependency	Kebergantungan antar node, arah panah mengarah pada node yang dipakai

#### 4. Componen Diagram

No	Simbol	Nama	Keterangan
1		Package	<i>sebuah bungkusian dari satu atau Lebih komponen</i>
2		Component	<i>komponen sistem</i>
3		interface	<i>Antarmuka komponen</i>
4		Dependency	Kebergantungan antar <i>komponen</i> , arah panah mengarah pada <i>komponen</i> yang dipakai

## DAFTAR LAMPIRAN

Lampiran 1 Surat Pengantar Riset.....	62
Lampiran 2 Surat Balasan Riset.....	63
Lampiran 3 Kartu Bimbingan Skripsi.....	64
Lampiran 4 Surat Keterangan Hasil Deteksi Plagiasi.....	65
Lampiran 5 Biodata Penulis Skripsi.....	66
Lampiran 6 Dataset NSL-KDD train.....	67
Lampiran 7 Data Hasil Capture Log Jaringan Wifi.id ISB Atma Luhur.....	68

