

DETEKSI SERANGAN DDOS (*DISTRIBUTED DENIAL OF SERVICE*) DI CLOUD COMPUTING DENGAN METODE RULE BASE



OLEH :

**RANDA FRATELLI JUNAEDI
09011181419006**

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019**

DETEKSI SERANGAN DDOS (*DISTRIBUTED DENIAL OF SERVICE*) DI CLOUD COMPUTING DENGAN METODE RULE BASE

TUGAS AKHIR

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



OLEH :

**RANDA FRATELLI JUNAEDI
09011181419006**

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019**

LEMBAR PENGESAHAN

DETEKSI SERANGAN DDOS (*DISTRIBUTED DENIAL OF SERVICE*) DI CLOUD COMPUTING DENGAN METODE RULE BASE

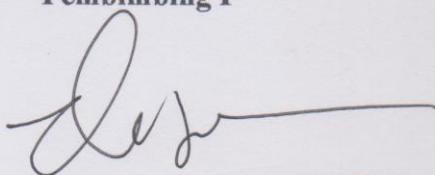
PROPOSAL TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

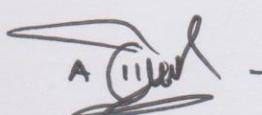
Randa Fratelli Junaedi
09011181419006

Pembimbing I



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

Indralaya, Juli 2019
Pembimbing II



Ahmad Heryanto,S.Kom., M.T.
NIP.198701222015041002

Mengetahui,
Ketua Jurusan Sistem Komputer



Rossi Passarella, S.T., M.Eng.
NIP.197806112010121004

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada : Ira Pratelli Junaidi

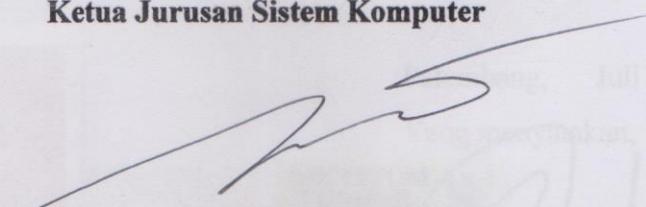
Hari : Sabtu
Tanggal : 20 Juli 2019

Tim Penguji :

1. Ketua : **Huda Ubaya, M.T**
2. Anggota I : **Dr. Reza Firsandaya Malik, M.T**
3. Anggota II : **Rahmad Fadli, M.Sc**

Demikianlah Penyajian ini saya buat dengan sebenarnya dan

Mengetahui,
Ketua Jurusan Sistem Komputer


Rossi Passarella, M.Eng.
NIP. 197806112010121004

HALAMAN PERNYATAAN

Yang bertandatangan di bawah ini :

Nama : Randa Fratelli Junaedi
NIM : 09011181419006
Program Studi : Sistem Komputer
Judul Skripsi : Deteksi serangan DDoS (*Distributed Denial of Service*)
Di *cloud computing* dengan metode *rule base*

Hasil Pengecekan *Software iThenticate/Turnitin* : 6 %

Menyatakan bahwa tugas akhir ini merupakan hasil karya saya sendiri dan bukan merupakan duplikasi maupun plagiasi (jiplakan) dari penelitian orang lain. Apabila tugas akhir ini terbukti merupakan hasil duplikasi atau plagiasi (jiplakan) dari hasil penelitian orang lain, maka saya bersedia menerima sanksi yang diberikan oleh Tim pengujian dan jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Demikian Surat Pernyataan ini saya buat dengan sebenar-benarnya.



Palembang, Juli 2019

Yang menyatakan,



Randa Fratelli Junaedi

NIM 09011181419006

HALAMAN PERSEMBAHAN

يَكَانُوا الَّذِينَ إِذَا مَنَّا لَهُمْ تَفَسَّحُوا فِي الْمَجَالِسِ فَأَفْسَحُوا
يَفْسَحُ اللَّهُ لَهُمْ وَإِذَا قِيلَ أُنْشُرُوا فَأَنْشُرُوا يَرْفَعَ اللَّهُ الَّذِينَ إِذَا مَنَّا
مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَيْرٌ
11

"Hai orang-orang beriman apabila dikatakan kepadamu: "Berlapang-lapanglah dalam majlis", maka lapangkanlah niscaya Allah akan memberi kelapangan untukmu. Dan apabila dikatakan: "Berdirilah kamu", maka berdirilah, niscaya Allah akan meninggikan orang-orang yang beriman di antaramu dan orang-orang yang diberi ilmu pengetahuan beberapa derajat. Dan Allah Maha Mengetahui apa yang kamu kerjakan."

(Q.S. Al-Mujadilah : 11)"

فَإِنَّ مَعَ الْعُسْرِ يُسْرًا

"Karena sesungguhnya sesudah kesulitan itu ada kemudahan"

Karya Besar Ini Kupersembahkan Kepada :

- Kedua orang tua-ku yang aku sayangi dan aku cintai. (Bapak Muhamad Edi, S.Pd & Ibu Junainah, S.Pd)
- Saudara Laki-laki-ku (Rendy Junaidi Macnis, S.Pd & Reval Diansyah Junaedi) dan Saudari Perempuan-ku (Indah Pratiwi Junaedi) Serta Keluarga besar-ku yang selalu memberikan motivasi.
- Keluarga Besar Sistem Komputer
- Teman-Teman Seperjuangan di Sistem Komputer 2014
- Almamaterku

KATA PENGANTAR

Puji syukur penulis haturkan kehadiran Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul **“Deteksi Serangan DDoS (*Distributed Denial of Service*) Di Cloud Computing Dengan Metode Rule Base”**. Shalawat dan salam tak lupa kita junjungan kepada Nabi kita Rasulullah SAW beserta keluarga, sahabat dan para pengikutnya hingga akhir zaman.

Pada kesempatan ini, penulis menyampaikan ucapan terima kasih kepada semua pihak yang telah memberikan segala kemudahan, bimbingan, pengarahan, dorongan, bantuan baik moril maupun materil selama penyusunan tugas akhir ini. Untuk itu penulis mengucapkan banyak terimakasih kepada :

1. Allah SWT yang telah memberikan segalanya kepada penulis berupa nikmat kesehatan, iman, dll sehingga penulis dapat menyelesaikan tugas akhir ini.
2. Keluarga besar tercinta, Bapak Muhammad Edi, S.Pd, Ibu Junainah, S.Pd, Aak Rendy, Koyong Reval, Kopek Indah, Yuk Dewi, Afif, Kakek, Nenek, Woh, Bibik, Oom, Mamang, Aak, Teteh, dan Sepupu semua, yang selalu ada dan tidak pernah lelah dalam mendidik serta memberikan dukungan baik secara moril maupun materil kepada penulis demi lancarnya tugas akhir ini.
3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

4. Bapak Rossi Passarella, S.T., M.Eng. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, Ph.D. dan Bapak Ahmad Heryanto, M.T. selaku Dosen Pembimbing tugas akhir. Dan Bapak Rossi Passarella, S.T., M.Eng. selaku pembimbing akademik, yang telah memberikan bimbingan dan semangat kepada penulis dalam menyelesaikan tugas akhir.
6. Bapak Dr. Reza Firsandaya Malik, M.T., Bapak Rahmad Fadli, M.Sc. selaku dosen penguji tugas akhir dan Bapak Huda Ubaya, M.T., selaku ketua sidang, yang telah memberikan kritik dan saran serta ilmu yang bermanfaat sehingga tulisan ini menjadi lebih baik.
7. Seluruh Dosen Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
8. Mba Winda, selaku admin jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
9. Seluruh Staf pegawai Fakultas Ilmu Komputer Universitas Sriwijaya yang telah membantu penyelesaian proses administrasi.
10. Kak Eko Arip Winanto, S.Kom., dan kak Candra Adi Winanto, S.Kom., yang telah mengajari proses-proses penggeraan tugas akhir dan memberikan motivasi serta semangat dalam menyelesaikan tugas akhir.
11. Para sahabat HsH Group Aidil Fitri Yansya, Yonatan Riyadhi, Sigit Wijaya Pramono, Gonewaje, Anggit Mardian, Ahmad Ridwan, Fahron, Fadli Nurhuda, Ade Rahmad, Hidayat, Ageng, Ega Aldo, Faris Nabil, Anshori, Epriyadi, dan teman-teman yang tidak dapat disebutkan satu

persatu yang telah membantu dalam proses belajar, memberikan canda tawa motivasi serta semangat pada tugas akhir ini.

12. Kakak-kakak Laboratorium COMNETS RG yang telah banyak berbagi cerita dan pengalaman : Kak Eko Arip, S.Kom, Kak Candra, S.Kom, Kak Johan Wahyudi, CND, Kak Riki Andika, S.Kom, Kak Dimas Wayudi, S.Kom, Kak Deni, S.Kom, Kak Bram, S.Kom, Kak Fepiliana, S.Kom, Kak Sri, S.Kom, Kak Leni, S.Kom.
13. Seluruh teman-teman angkatan 2014 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
14. Serta semua pihak yang telah membantu baik moril maupun materil yang tidak dapat disebutkan satu persatu dalam penyelesaian tugas akhir ini.
Terima Kasih Semuanya.

Semoga dengan terselesainya tugas akhir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua. Dalam penulisan laporan ini penulis menyadari bahwa masih ada banyak kekurangan dan ketidak sempurnaan, oleh karena itu penulis mohon kritik dan saran yang membangun untuk Perbaikan Laporan Tugas Akhir ini, agar menjadi lebih baik dimasa yang akan datang.

Indralaya, Juli 2019

Penulis

Distributed Denial of Service (DDoS) Detection on Cloud Computing using the Rule Base Method

Randa Fratelli Junaedi (09011181419006)

Department of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email: Randafratelli93@gmail.com

ABSTRACT

Distributed Denial of Service is a type of attack that is generated by many sources that are distributed simultaneously by overloading bandwidth on the target server. *SYN Flood Attack Distributed Denial of Service* aims to spend resources by sending many *SYN request* package to target machines. The SYN Flood attack was found based on Snort IDS from the dataset resulting from a SYN Flood attack in the form of raw data (pcap file). From these results, information is obtained in the form of alerts that will be needed in determining the attack pattern for the detection process by applying the *Rule-Based Signature* method in the *Python Algorithm*. From the results of the detection, the value of *True Positive Rate* was 95.6%, while the value of *False Negative Rate* was 4.4%, and *Accuracy* was 95.6%.

Keywords: *Distributed Denial of Service, SYN Flooding, rule based signature.*

Deteksi Serangan DDoS (Distributed Denial of Service) di Cloud Computing dengan Metode Rule Base

Randa Fratelli Junaedi (09011181419006)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email : Randafratelli93@gmail.com

ABSTRAK

Distributed Denial of Service merupakan jenis serangan yang dihasilkan oleh banyak sumber yang didistribusikan secara bersamaan dengan cara membebani *bandwidth* pada target server. Serangan *SYN Flood Distributed Denial of Service* bertujuan untuk menghabiskan sumber (*resource*) dengan cara mengirimkan banyak paket *SYN request* terhadap mesin sasaran. Ditemukan adanya serangan *SYN Flood* berdasarkan *IDS Snort* dari dataset hasil percobaan serangan *SYN Flood* berupa raw data (file pcap). Dari hasil tersebut didapatkan informasi berupa alert yang akan dibutuhkan dalam menentukan pola serangan untuk proses deteksi dengan menerapkan metode *Rule-Based Signature*. Dari hasil deteksi didapatkan nilai *True Positive Rate* sebesar 95,6% sedangkan nilai *False Negative Rate* diperoleh nilai sebesar 4,4%, dan didapatkan nilai *Accuracy* sebesar 95,6%.

Kata Kunci : *Distributed Denial of Service, SYN Flooding, rule based signature.*

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
LEMBAR PENGESAHAN	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PERNYATAAN	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
ABSTRACT	ix
ABSTRAK	x
DAFTAR ISI	xi
DAFTAR GAMBAR	xiv
DAFTAR TABEL	xv
BAB I. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Tujuan	2
1.3 Manfaat	2
1.4 Rumusan Masalah	3
1.5 Batasan Masalah.....	3
1.6 Metodologi Penelitian	3
1.7 Sistematika Penelitian	4
BAB II. TINJAUAN PUSTAKA.....	6
2.1 Diagram Konsep Penelitian.....	6
2.2 Intrusion Detection System (IDS)	7
2.3 Arsiterktur Intrusion Detection System (IDS)	7
2.4 Klasifikasi (IDS) Berdasarkan Deployment.....	8
2.4.1 Network-based Intrusion Detection System (NIDS).....	9
2.4.2 Host-based Intrusion Detection System (HIDS)	9

2.5 Klasifikasi (IDS) Berdasarkan Metode Deteksi.....	9
2.5.1 Signature-based Detection IDS	9
2.5.2 Anomaly-based Detection IDS	10
2.5.3 Hybrid-Based Detection IDS	10
2.6 Klasifikasi IDS Berdasarkan Waktu Pemeriksaan.....	11
2.6.1 Offline Intrusion Detection System	11
2.6.2 Real-Time Intrusion Detection System.....	11
2.7 Klasifikasi IDS Berdasarkan Struktur Sistem.....	11
2.7.1 Centralized Intrusion Detection System.....	12
2.7.2 Distributed Intrusion Detection System	12
2.8 Distibuted Denial of Service Attack	12
2.8.1 Karakteristik Serangan Distibuted Denial of Service	13
2.8.2 Jenis - Jenis Serangan Distibuted Denial of Service.....	14
2.9 SYN Flooding	14
2.10 Confusion Matrix	15
2.11 Cloud Computing	16
2.12 Data Ekstaction	18
 BAB III. METODOLOGI	 19
3.1 Pendahuluan	19
3.2 Kerangka Kerja Penelitian	19
3.3 Perancangan Sistem	21
3.3.1 Perancangan Topologi.....	21
3.3.2 Kebutuhan Perangkat Keras (Hardware)	22
3.3.3 Kebutuhan Perangkat Lunak (Software).....	23
3.4 Skenario Pembuatan Dataset.....	23
3.5 Data Extraction.....	25
3.6 Snort sebagai NIDS.....	26
3.7 Mengenali Pola Serangan SYN Flood	28
3.8 Rule-Based Signature.....	30

BAB IV. HASIL DAN PEMBAHASAN	31
4.1 Pendahuluan	31
4.2 SYN Flood Distributed Denial of Service Attack.....	31
4.3 Analisa Dataset.....	32
4.4 Hasil Data Extraction	33
4.5 Validasi Hasil Data Extraction.....	34
4.6 Pengenalan Pola Serangan SYN Flood DDoS	36
4.7 Validasi alert snort, rules snort, dan data extraction	38
4.8 Pengujian Sistem deteksi menggunakan metode rule base.....	39
BAB V. KESIMPULAN	44
Daftar Pustaka	46

DAFTAR GAMBAR

	Halaman
2.1. Diagram konsep penelitian	6
2.2. Arsitektur dasar IDS[8]	7
2.3. Klasifikasi IDS berdasarkan Deployment	8
2.4. Ilustrasi dari serangan Distributed Denial of Service	13
3.1. Kerangka kerja penelitian	20
3.2. Topologi dataset serangan SYN Flood DDoS	21
3.3. Topologi terjadinya serangan SYN Flood DDoS	24
3.4. Rules Snort SYN Flood DDoS[20]	27
3.5. Hubungan Alert, Raw Data, hasil Data Extraction	29
3.6. Flowchart Rule-Based Signature	30
4.1. Command SYN Flood DDoS Attack	31
4.2. Grafik traffic dan jumlah paket data pada dataset	33
4.3. Hasil ekstraksi data serangan dan normal	34
4.4. Validasi raw data dan hasil data extraction	35
4.5. Pencocokan alert snort dan hasil data extraction	37
4.6. Validasi alert snort, rules snort, dan data extraction	38
4.7. Hasil pengujian menggunakan metode rule base pada data gabungan	40
4.8. Validasi raw data pcap dengan pengujian rule base	40
4.9. Grafik traffic Binary Classification dari data gabungan	42
4.10. Grafik traffic Detection Rate	43

DAFTAR TABEL

	Halaman
Tabel 2.1. Tipe alert pada confusion matrix	15
Tabel 2.2. Confusion matrix.....	16
Tabel 3.1. Spesifikasi kebutuhan perangkat keras	22
Tabel 3.2. Spesifikasi kebutuhan perangkat lunak.....	23
Tabel 3.3. Skenario pengujian serangan SYN Flood DDoS	25
Tabel 3.4. Atribut data extraction	26
Tabel 4.1. Dataset yang digunakan	32
Tabel 4.2. Jumlah paket serangan, normal, dan gabungan pada dataset.....	33
Tabel 4.3. Atribut pola serangan SYN Flood DDoS Attack	38
Tabel 4.4. Data pola yang digunakan pada metode rule base	39
Tabel 4.5. Confusion Matrix	41
Tabel 4.6. Nilai persentase Detection rate confusion matrix	42

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Serangan DoS (Denial of Service) adalah jenis serangan, terhadap suatu komputer atau server di dalam suatu jaringan internet dimana dengan cara menghabiskan sumber (resource) yang dimiliki oleh suatu komputer, sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar. sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang. DDoS (Distributed Denial of Service) adalah salah satu jenis serangan Denial of Service yang menggunakan banyak host penyerang (baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang dipaksa menjadi zombie) untuk menyerang satu buah host target dalam sebuah jaringan.

Menurut [1], Serangan DDoS adalah serangan DoS yang dihasilkan oleh banyak sumber yang didistribusikan secara bersamaan. Penyerang menggunakan worm dan virus untuk menginfeksi perangkat yang akan digunakan dalam serangan.

Dalam penelitian sebelumnya [2], Distributed Denial of Service (DDoS) adalah serangan yang menghabiskan semua sumber daya cloud dan mungkin membuatnya tidak tersedia untuk pengguna umum lainnya. Tujuan serangan ini adalah untuk 'membebani' bandwidth server, dan sumber daya lainnya, sehingga siapa pun tidak bisa untuk mendapatkan akses ke server. Serangan DDoS (Distributed Denial of Service) hampir sama dengan serangan DoS, tetapi hasil serangan DDoS lebih besar. Serangan DDoS dieksekusi menggunakan metode komputasi terdistribusi yang sering disebut 'botnet army', proses pembuatannya dengan menginfeksi komputer dengan bentuk malware yang memberikan pemilik botnet akses ke komputer.

Pada penelitian sebelumnya [3], [4], juga membahas tentang sistem deteksi serangan *Denial of Service*, dimana teknik yang digunakan, Earth Mover's

Distance (EMD) dan Multivariate Correlation Analysis (MCA), teknik penelitian tersebut berbeda akan tetapi tujuan dari apa yang dilakukan sama-sama untuk mendeteksi serangan *Denial of Service*.

Dalam Penelitian [5], DDoS adalah serangan terkoordinasi, yang menggunakan beberapa mesin untuk meluncurkan serangan, bukan satu mesin. Dalam jenis serangan DDoS, penyerang menggunakan botnet, yang merupakan jaringan host yang disusupi, untuk meluncurkan serangan. Karena keterlibatan beberapa mesin, sangat sulit untuk menemukan sumber serangan dan mengurangi serangan. Serangan DDoS dapat diklasifikasikan ke dalam dua kategori, berbasis lapisan jaringan dan berbasis lapisan aplikasi. Serangan berbasis lapisan jaringan, menggunakan protokol lapisan jaringan dan transport untuk flooding yaitu TCP, UDP dan IP. Serangan berbasis lapisan aplikasi, menggunakan pesan XML dan HTTP yang cacat.

Berdasarkan latar belakang masalah tersebut, maka pada penelitian tugas akhir ini penulis akan melakukan pendekripsi serangan *Distributed Denial of Service* dan metode *Rule Base* dicloud atau mengkategorikan pola *traffic* data serangan maupun data normal.

1.2 Tujuan

Adapun tujuan dari penelitian ini yaitu :

1. Mengenali pola serangan SYN Flood *DDoS*
2. Membuat algoritma untuk mendeteksi paket serangan *Distributed Denial of Service* di cloud
3. Menerapkan metode *Rule Base* untuk mengelompokkan trafik serangan maupun trafik normal.
4. Mendeteksi serangan *Distributed Denial of Service* dalam suatu jaringan cloud.

1.3 Manfaat

Adapun manfaat yang dapat diambil dari penelitian ini adalah:

1. Dapat memberikan kemudahan dalam mengenali serangan SYN Flood *DDoS* dalam suatu jaringan cloud.

2. Dapat mengetahui pola paket data serangan SYN Flood *DDoS* dan pola paket data normal.

1.4 Perumusan Masalah

Berikut ini merupakan perumusan masalah dalam penelitian ini :

1. Bagaimana cara mengenali pola paket data serangan SYN Flood *DDoS* maupun paket data normal dalam suatu jaringan cloud.
2. Bagaimana mengelompokkan trafik serangan maupun trafik normal pada serangan *Distributed Denial of Service* menggunakan metode *Rule Base*.

1.5 Batasan Masalah

Berdasarkan rumusan masalah diatas, berikut ini merupakan batasan masalah pada penyusunan tugas akhir ini :

1. Data serangan pada penelitian berfokus pada *Distributed Denial of Service* SYN Flooding.
2. Paket data serangan akan dikelompokkan kedalam dua bagian, yaitu *traffic* normal dan *traffic* serangan.
3. Metode yang digunakan untuk mengelompokkan data yaitu *Rule Base*.
4. Tidak membahas tentang bagaimana cara pencegahan serangan *Distributed Denial of Service*

1.6 Metodologi Penelitian

Dalam tugas akhir ini terdapat beberapa metodologi yang digunakan, antara lain yaitu :

1. Studi Pustaka

Pada tahap pertama ini yang dilakukan yaitu studi pustaka atau *literature*. Pada tahap ini dapat mempelajari dan mengumpulkan informasi tentang penelitian yang akan dilakukan, studi pustaka ini bisa diperoleh dari jurnal-jurnal, buku, atau artikel mengenai penelitian yang akan dikerjakan.

2. Perancangan Sistem

Pada tahap kedua ini membahas tentang proses bagaimana membangun dengan menggunakan metode atau pendekatan tertentu. Kemudian menentukan

jenis perangkat keras dan perangkat lunak yang digunakan dalam penelitian, juga jenis topologi yang digunakan, dan jenis bahasa pemrograman yang digunakan di dalam sistem. Selain itu penerapan metode yang digunakan pada penelitian tugas akhir ini.

3. Pengujian

Pada tahap ketiga ini melakukan pengujian berdasarkan dengan metodologi penelitian dan juga penelitian sebelumnya sehingga menghasilkan hasil uji yang sesuai dengan parameter yang sudah ditentukan .

4. Analisa

Pada tahap ini menganalisa hasil dari pengolahan data pada tahap sebelumnya. Bertujuan untuk memperoleh data secara objektif dari analisa hasil pengolahan data guna dapat dikembangkan lagi pada penelitian selanjutnya.

5. Kesimpulan dan Saran

Selanjutnya dilakukan penarikan kesimpulan dalam penulisan penelitian tugas akhir. Pada tahap ini terdapat juga beberapa saran yang dapat digunakan untuk penelitian selanjutnya.

1.7 Sistematika Penelitian

Pada tugas akhir ini di buat sistematika penelitian agar mempermudah dalam proses penyusunan dan memperjelas isi dari setiap bab sebagai berikut :

BAB I. PENDAHULUAN

Bab ini berisi tentang penjelasan mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah, Batasan Masalah, Metodologi Penelitian, dan Sistematika Penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini berisi teori tentang penelitian yang akan dilakukan seperti, *Intrusion Detection System*, *Cloud Computing*, *Distributed Denial of Service*, dan teori lainnya yang berhubungan dengan penelitian.

BAB III. METODOLOGI PENELITIAN

Bab ini berisi tentang penjelasan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini yaitu mengenai tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV. PENGUJIAN DAN ANALISA

Bab ini menjelaskan hasil pengujian yang dilakukan serta analisis dari tiap data yang diperoleh dari hasil pengujian berdasarkan batasan masalah dan parameter yang sudah ditentukan.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan tentang hasil penelitian yang telah dilakukan, apakah hasilnya sesuai dengan tujuan yang tercantum pada BAB I. Serta berisi saran-saran untuk penelitian selanjutnya.