PENGENALAN POLA SERANGAN *DENIAL OF SERVICE* (*UDP FLOOD)* PADA JARINGAN *INTERNET OF THINGS (IOT)* DENGAN ALGORITMA *DECISION TREE* C4.5

OLEH:

RIKI ANDIKA
09011181320015

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2018

PENGENALAN POLA SERANGAN *DENIAL OF SERVICE* (*UDP FLOOD)* PADA JARINGAN *INTERNET OF THINGS (IOT)* DENGAN ALGORITMA *DECISION TREE* C4.5

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH:

RIKI ANDIKA
09011181320015

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018

LEMBAR PENGESAHAN

PENGENALAN POLA SERANGAN *DENIAL OF SERVICE (UDP FLOOD)* PADA *JARINGAN INTERNET OF THINGS (IOT)* DENGAN ALGORITMA *DECISION TREE C4.5*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

RIKI ANDIKA
09011181320015

Palembang, Desember 2018

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng.
NIP. 197806112010121004

Pembimbing

Deris Stiawan, Ph.D.
NIP. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Sabtu
Tanggal : 24 November 2018

Tim Penguji :

1. **Ketua : Ahmad Zarkasi, M.T.** _____
2. **Anggota I : Dr. Reza Firsandaya Malik, M.T.** _____
3. **Anggota II : Rido Zulfahmi, M.T.** _____

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M.Eng.
NIP. 197806112010121004

HALAMAN PERNYATAAN

Yang bertandatangan dibawah ini :

Nama	: Riki Andika
NIM	: 09011181320015
Program Studi	: Sistem Komputer
Judul Skripsi	: Pengenalan Pola Serangan *Denial of Service (UDP Flood)* pada Jaringan *Internet of Things (IoT)* dengan Algoritma *Decision Tree C4.5*

Hasil Pengecekan *Software iThenticate/Turnitin* : 19%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain . Apabila ditemukan unsur penjiplakan / plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik yang diberikan oleh Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Demikian Pernyataan ini saya buat dengan sebenar-benarnya.

Palembang, Desember 2018

Yang menyatakan,

METERAI TEMPEL
TGL 20
DE877AFF480534120
6000
ENAM RIBU RUPIAH

Riki Andika
NIM. 09011181320015

HALAMAN PERSEMBAHAN

*"Terlambat **lulus** atau **lulus** tidak tepat waktu bukanlah sebuah kejahatan, bukan sebuah aib, bukan pula sebagai bahan cemoohan (pengucilan). Alangkah kerdilnya jika mengukur kepintaran seseorang hanya dari siapa yang paling cepat **lulus**. Bukankah sebaik-baiknya **skripsi** adalah **skripsi** yang selesai dan yang diselesaikan sendiri? Baik itu selesai tepat waktu maupun tidak tepat waktu semuanya ada pada diri kita sendiri, tapi ingatlah semuanya akan indah pada waktu yang tepat."*

يَا أَيُّهَا الَّذِينَ آمَنُواْ اسْتَعِينُواْ بِالصَّبْرِ وَالصَّلاَةِ إِنَّ اللّهَ مَعَ الصَّابِرِينَ

Artinya : *"Hai orang-orang yang beriman, jadikanlah sabar dan shalat sebagai penolongmu, sesungguhnya Allah beserta orang-orang yang sabar."*
(QS. Al-Baqarah [2]: 153).

Dengan mengucap syukur Alhamdulillah atas rahmat Allah Subhanahu wa Ta'ala, kupersembahkan karya kecil ini untuk . . .

Kedua orang tua tercinta

(Bapak Jumadi Salim dan Ibu Suwa Matnahir)

Keempat kakak perempuan ku,

(Linsi Satralia, Linsa Maryani, Lipi Suwarni, Liska Juarni Damayanti)

Teman-teman seperjuangan jurusan,

(Sistem komputer angkatan 2013)

Teman-teman organisasi,

(Lab COMNETS, LDF WIFI, BEMF, dan IMMETA)

Almamater perjuangan

(Universitas Sriwijaya)

20 Desember 2018

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan rahmat, hidayah serta ijin-Nya sehingga penulis dapat menyelesaikan penulisan tugas akhir dengan judul **"Pengenalan Pola Serangan *Denial of Service (UDP Flood)* pada Jaringan *Internet of Things (IoT)* dengan Algoritma *Decision Tree C4.5*"**. Penulisan tugas ahir ini dibuat dalam rangka memenuhi persyaratan untuk menyelesaikan pendidikan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya untuk memperoleh gelar strata 1.

Pada kesempatan ini, penulis menyampaikan ucapan terima kasih kepada semua pihak untuk setiap bimbingan, semangat dan doa yang diberikan kepada penulis sehingga terselesaikannya tugas akhir ini. Ucapan terima kasih, penulis sampaikan kepada:

1. Allah SWT, yang telah memberikan segalanya kepada penulis berupa kesehatan, orang tua, pembimbing, teman, dll sehingga dapat menyelesaikan laporan tugas akhir ini.
2. Orang-orang tercinta, Ayah, Ibu, Kakak-kakak perempuan, kakak-kakak ipar serta ponakan-ponakan tersayang, yang selalu ada dan tidak pernah lelah dalam mendidik serta memberikan dukungan baik secara moril maupun materil kepada penulis demi lancarnya penulisan tugas akhir ini.
3. Bapak Dr. Deris Stiawan, Ph. D selaku Dosen Pembimbing tugas akhir, yang telah memberikan bimbingan dan semangat kepada penulis dalam menyelesaikan tugas akhir.
4. Bapak Dr. Reza Firsandaya Malik, M.T dan Bapak Rido Zulfahmi, M.T selaku dosen penguji sidang tugas akhir yang telah memberikan kritik dan saran serta ilmu yang bermanfaat sehingga tulisan ini menjadi lebih baik.
5. Bapak Firdaus, M.Kom selaku Pembimbing Akademik, yang telah membimbing penulis dari semester satu hingga terselesainnya tugas ahir ini dengan baik.
6. Bapak Rossi Passarella, M.Eng selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

7. Seluruh Dosen Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Univeristas Sriwijaya.
8. Staff di jurusan Sistem Komputer, khususnya Kak Ahmad Reza yang telah membantu penyelesaian proses administrasi.
9. Staff di Fakultasi Ilmu Komputer, bagian akademik, kemahasiswaan, tata usaha, perlengkapan, dan keuangan, yang telah membantu penyelesaian proses administrasi.
10. Seluruh petinggi atau pimpinan yang ada dilingkungan Fakultas Ilmu Komputer, Universitas Sriwijaya, yang telah membantu proses administrasi selama masa kampus.
11. Teman-teman satu tema dalam penelitian ini dikeamanan jaringan *internet of things (IoT),* Dimas Wahyudi S.Kom, Meilinda Eka Suryani S.Kom, serta kak kgs Rahmat Shaleh, S.Kom (segera).
12. Teman-teman Laboratorium COMNETS yang telah banyak membagi ceritanya Johan Wahyudi, S.Kom (segera), Rendika Adha Tanjung, S.Kom (segera), Dimas Wahyudi, S.Kom, Kak Deni Danuarta, S.Kom, Kak M Dimas Firmansyah, S.Kom, Kak Ahmad Zaki, S.Kom, Sri Suryani, S.Kom, Fepiliana, S.Kom, Meilinda Eka Suryani, S.Kom, Leny Novita Sari, S.Kom, Resti Handayani,S.Kom (segera), Kristiawati Ginting, S.Kom (segera), Ahmad Ridwan, S.Kom (segera), Aidil Fitriyansyah, S.Kom (segera), Gone Wajeh, S.Kom (segera), Anggit Mardian, S.Kom (segera), Serta semua penghuni Laboratorium lantai 2 .
13. Kakak-kakak super duper yang telah memberikan motivasi dan masukan-masukannya, Kak Eko Arif Winanto, S.Kom, Kak Candra Adi Winanto, S.Kom, Kak Apriadi, S.Kom sehingga terselesainya tugas ahir ini diwaktu yang tepat.
14. Teman-teman satu kosan (EG55) yang telah memberikan waktu, cerita, pengalaman dalam penyelesaian tugas ahir ini, Andi Agusta, S.SI (segera), Ahmad Supaidi,S.SI (segera) dan Muhamad Yusup, S.Kom (segera).
15. Teman-Teman bisnis di JUKITA yang ketche-ketche Andi Agusta, S.SI (segera), Zefta Adetya, S.SI (segera), Meila Kusuma Perdana, S.Kom (segera),

Bella Pertiwi, S.Kom (segera), Destiana Pramasari, S.Kom (segera), Alviansyah S.Kom (segera).

16. Teruntuk teman-teman satu angkatan, khususnya Sistem Komputer kelas A, Eko Pratama, S.Kom (ketua kelas), Andhika Riski Perdana, S.Kom, Erick Okvanty Haris, S.Kom, Tri Atmoko Malik Kurniawan, Imam Mustofa, Ahmad Kuswandi, Yoppy Prayudha, Ryan Fitrah Perdana, Dwi Kurnia Putra, Dede Tri Septiawan, Faris Abdul Aziz, Sandi Sarfani, Agus Juliansyah, Fahrul Rozi, M F Ilham Saputra, Yayang Paryoga, Kholil Anggara, Rio Astani, Adi Suryan, Sri Suryani, S.Kom, Fepiliana, S.Kom, Leny Novita Sari, S.Kom, Meilinda Eka Suryani, S.Kom, Ulan Purnamasari, S.Kom, Umi Yanti, S.Kom, Indah Sari, Nova Dyati Pradista, Lisa Mardaleta, Nur Rahma Dela, Saros Sakiana, Kusuma Dwi Indriani, Elfa Purnamasari, Suci Anggraini. Semoga lekas sidang juga, sukses untuk kita semua.
17. Serta Organisasi diFakultas Ilmu Komputer maupun Universitas Sriwijaya, LDF WIFI (Lembaga Dakwah Fakultas Wahana Islamiyah dan Forum Ilmu), HIMASISKO (Himpunan Mahasiswa Sistem Komputer), BEM F (Badan Eksekutif Mahasiswa Fakultas), NAC (Network Administrator Club), KAMMI AL AQSHA (Kesatuan Aksi Mahasiswa Muslim Indonesia), HTI Palembang (Hizbut Tahrir regional Pelembang), kedaerahan IMMETA SUMSEL (Ikatan Mahasiswa Kabupaten Muara Enim Sumatera Selatan), KADIKSRI (Keluarga Mahasiswa BIDIKMISI Universitas Sriwijaya), terima kasih atas kesempatannya dalam menjadi keluarga besar, atas ilmu yang telah diberikan serta wadah berbagi yang hangat.
18. Serta semua pihak yang telah membatu baik moril maupun materil yang tidak dapat disebutkan satu persatu dalam penyelesaian tugas ahir ini. Terima kasih semuanya.

Semoga dengan terselesainya tugas ahir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua dalam mempelajari deteksi serangan *Denial of Sevice (UDP Flood)* pada jaringan *Internet of Thing* dengan menggunakan algoritma *Dicision tree C4.5.*

Dalam Penulisan laporan ini penulis juga sangat menyadari bahwa masih banyak terdapat kekurangan dan ketidak sempurnaan, oleh karena itu penulis mohon saran dan kritik yang membangun untuk Perbaikan Laporan Tugas Akhir ini, agar menjadi lebih baik dimasa yang akan datang.

Palembang, Desember 2018

Penulis

Recognition of Denial of Service (UDP Flood) Patterns on the Internet of Things (IoT) Network with the Decision Tree C4.5 Algorithm

Riki Andika (09011181320015)
Departement of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email: rikiandika57@gmail.com

Abstract

Recognition of attack pattern is one of the way that can be used to be able to detect attacks that occur on the network. The attacks can be identified by pattern is the denial of service (udp flood) that occurs on the internet of things, the internet of things network built in this research has seven nodes with sensor data which is then sent to the server, using the protocol and xbee protocol. Denial of service attack (upd flood) is a connectionless attack that floats so it can make the network busy with abnormal traffic. The pattern of denial service (udp flood) can be identified by several parameters such as IP time to live, IP length, UDP length and payload. In this research using the C4.5 decision tree algorithm that is used to classify normal data and attack data to obtain effective results with the final research obtained an accuracy value of 99.98% precision of 99.99% and a recall value of 100%.

Keywords: *C4.5 decision tree, Denial of service, Flood, Internet of things, Pattern Recognition.*

Pengenalan Pola Serangan *Denial of Service (UDP Flood)* pada Jaringan *Internet of Things (IoT)* dengan *Algoritma Decision Tree C4.5*

Riki Andika (09011181320015)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: rikiandika57@gmail.com

Abstrak

Fokus penelitian ini ialah deteksi serangan *denial of service (UDP flood)*, dengan mengenali pola dari serangan *denial of service (UDP flood)* yang terjadi pada jaringan *internet of things*, jaringan *internet of things* yang dibangun dalam penelitian ini memiliki enam node dengan memiliki sensor pada setiap nodenya, dimana setiap sensor akan melakukan pembacaan data sensor yang kemudian akan dikirimkan ke *server*, dengan menggunakan komunikasi *wifi* dan *xbee.* Serangan *denial of service (udp flood)* merupakan serangan yang bersifat *connectionless* yang melakukan *flooding* sehingga dapat membuat jaringan menjadi sibuk dengan *traffic* yang tidak normal. Pola serangan *denial of service (udp flood)* dapat dikenali dengan beberapa parameter seperti *ip time to live, ip length, ip header length, udp length,* dan *payload* . Pada penelitian ini menggunakan *algoritma decision tree c4.5* yang digunkaan untuk klasifikasi data normal dan data serangan guna memperoleh hasil yang lebih efektif, dengan hasil ahir penelitian memperoleh nilai akurasi sebesar 99,98%, presisi sebesar 99,99% dan nilai recall sebesar 100%.

Kata Kunci : Pengenalan pola, *internet of things, denial of service, udp flood, decision tree c4.5*

DAFTAR ISI

BAB III METODELOGI

BAB IV HASIL DAN PEMBAHASAN

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR PERSAMAAN

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet of things (IoT), merupakan suatu konsep dimana benda-benda yang hadir dalam kehidupan manusia dapat terhubung pada internet yang dapat melakukan proses penerimaan dan mengirim data secara digital [1], dimana dapat di monitoring dan di kontrol dari kejauhan serta dapat melakukan pekerjaan-pekerjaan lainnya [2]. *Internet of things* (IoT) merujuk pada suatu penggunaan perangkat yang terhubung antar perangkat lainnya secara cerdas dan sistem dapat memperoleh data melalui *embeded* sensor atau *aktuator* pada suatu mesin dan objek fisik yang lain[1][3].

Paradigma dari *Internet of things* (IoT) ialah dengan adanya banyak objek yang terhubung pada suatu jaringan yang memiliki fungsi berbeda-beda. *Radio Frequency Identification* (RFID) dan teknologi sensor jaringan akan meningkat penggunaannya, sehingga data yang dihasilkan dari penggunaan tersebut semakin meningkat, membuat daya simpan menjadi besar, yang dapat diproses serta ditampilkan dalam bentuk yang lebih efisien dan mudah untuk diterjemahkan. Konektivitas cerdas dengan jaringan yang ada dan komputasi menggunakan sumber daya jaringan adalah bagian yang sangat diperlukan dalam *Internet of things* (IoT) [4] [5].

Sisi lain [6] [7] [8] menjelaskan mengenai analisa serta pengenalan pola serangan yang terjadi pada *Intrusion Detection System* (IDS), dimana dari analisa yang dilakukan terbentuk *rules* atau model yang dapat dijadikan pola untuk klasifikasi dari serangan yang ada pada *Intrusion Detection System* (IDS) sehingga *rules* ini dapat diterapkan pada implementasi sistem yang akan dibangun. Pendeteksian pada *Intrusion Detection System* (IDS) dengan menggunakan algoritma *minkowski K-Means* dan *Decision Tree* dimana *feature selection* dan *rules* yang diperoleh diklasifikasikan, sehingga memperoleh tingkat keakurasian deteksi sebesar 94,78%, dengan tingkat keakurasian yang

tinggi memperlihatkan bahwa algoritma tersebut dapat dijadikan sebagai rujukan [9] .

Selanjutnya pada penelitian [10] [11] yang membahas penerapan dari *Intrusion Detection System* dengan menggunakan jenis algoritma *Decision Tree*, pada penelitiannya menggunakan dua *variant* dari algoritma *decision tree* yang digunakan untuk membuat pohon keputusan dalam klasifikasi data *mining* yang diperoleh, dengan mendapatkan tingkat keakurasian yang sangat baik, yakni 98,45%. Algoritma *Decision tree c4.5* merupakan salah satu algoritma yang dapat digunakan untuk klasifikasi suatu *data mining* [12], dimana algoritma ini berfungsi atau bekerja dengan membuat suatu pohon keputusan (*decision tree*), algoritma *Decision tree c4.5* merupakan pengembangan dari algoritma ID3. *Decision tree* berguna untuk mengeksplorasi data dengan menggunakan hubungan yang tersembunyi antara variabel *input* dengan variabel target, dimana algoritma *Decision tree* C4.5 dengan *input* berupa tabel dan menghasilkan *output* berupa pohon keputusan.

Penelitian sebelumnya [10] menggunakan dua algoritma, dimana algoritma yang digunakan ialah algoritma *naive bayes* dan *decision tree*, yang digunakan untuk mengklasifikasi *data mining*, pada masing-masing algoritma yang digunakan menggunakan standar pengujian akurasi klasifikasi, presisi, analisis sensitivitas spesifitas, dengan melakukan sepuluh kali pengujian pada sepuluh *dataset* dari University of North Carolina (Universitas Calivornia, Irvine), sehingga hasil dari penggunaan dua algoritma klasifikasi ini baik untuk digunakan dalam mengklasifikasi *data mining*.

Dengan rujukan pada masing-masing penelitian sebelumnya, maka pada penelitian tugas ahir ini akan dilakukan klasifikasi serangan *Denial of service (UDP Flood)* pada jaringan *internet of things* dengan menggunakan algoritma *Decision Tree*, yang digunakan untuk mengkategorikan pola paket serangan pada jaringan *internet of things.* Penggunaan algoritma ini dengan harapan dapat mewujudkan suatu sistem yang dapat memberikan gambaran dari pengenalan pola dan deteksi serangan *Denial of service (UDP Flood)* dengan akurasi pendeteksian yang baik.

1.2 Tujuan

Adapun tujuan yang hendak di capai dalam penelitian tugas ahir ini adalah sebagai berikut :

1. Pengenalan pola serangan *UDP Flood* dari *Denial of service (DoS)* pada jaringan *Internet of things* (IoT)
2. Mengimplementasikan *Intrusion Detection System (IDS)* pada Jaringan *Internet of things (IoT)*.
3. Menerapkan *Intrusion Detection System* dengan menggunakan algoritma *Decision tree c4.5* dalam pengolahan data yang diperoleh (*klasifikasi*).

1.3 Manfaat

Adapun manfaat yang di dapat dari penelitian ini di antaranya adalah sebagai berikut :

1. Dapat mengenali pola serangan *UDP Flood* dari *Denial of service* (DoS) pada jaringan *Internet of things* (IoT)
2. Menerapkan *Intrusion Detection System* (IDS) di jaringan *Internet of things* (IoT) dengan menggunakan algoritma *Decision tree c4.5*.
3. Hasil ahir dari tugas ahir ini berupa deteksi serangan *UDP Flood* yang kemudian diklasifikasi dengan menggunakan algoritma *Decision tree c4.5*.

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah di tulis, didapatkan perumusan masalah sebagai berikut :

1. Bagaimana cara melakukan pengidentifikasian pengenalan pola serangan *UDP Flood* dari *Denial of service* (DoS) yang ada pada jaringan *Internet of things* (IoT).
2. Bagaimana membangun sistem *Intrution Detection System* (IDS) dan cara kerja dari sistem untuk mendeteksi serangan *UDP Flood* dari *Denial of service* (DoS) pada jaringan *Internet of Things* (IoT).
3. Bagaimana cara melakukan klasifikasi data yang telah diperoleh dengan menggunakan algoritma *Decision tree c4.5*.

1.5 Batasan Masalah

Batasan masalah pada tugas akhir ini antara lain adalah sebagai berikut :

1. Pengenalan pola serangan *UDP Flood dari Denial of service* (DoS) serta menjelaskan cara kerja dari serangan *Denial of service* (DoS).
2. Hanya membahas serangan *Denial of service* (DoS) terkhusus serangan *UDP Flood* dan tidak membahas cara atau teknik dari serangan lainnya.
3. Tidak membahas mengenai pencegahan terhadap serangan yang ada pada jaringan.
4. Mekanisme deteksi berasaskan *Statistical-based Detection*.
5. Algoritma yang di gunakan untuk mendeteksi serangan *Denial of service* (DoS) adalah algoritma *Decision tree c4.5* dalam pengolah data yang diperoleh (klasifikasi).
6. Sistem yang dibangun memiliki empat *node*, satu *router*, dan 1 (satu) *coordinator*.
7. Sensor yang di gunakan pada sisi *end node* adalah sensor suhu (DHT 22) dan sensor gas atau asap (MQ-2), sensor kelembaban tanah, sensor kedalaman air.
8. Pada setiap *end node* terdapat satu buah sensor yang digunakan.
9. Pengujian sistem di lakukan secara *realtime* tetapi tidak secara *online*.
10. Pengujian dilakukan dengan menggunakan *protocol* jaringan *wifi*

1.6 Metodologi Penelitian

Metodologi yang di gunakan dalam penelitian ini melalui beberapa tahapan, diantaranya adalah sebagai berikut :

1. Tahap Pertama (Perumusan Masalah)

   Pada tahap ini mengamati fenomena yang terjadi berkaitan dengan studi kasus yang dijadikan objek penelitian tugas akhir, dengan membuat perumusan dari permasalahan yang akan dibuat dalam penyelesaian tugas ahir ini.
2. Tahap Kedua (Studi Pustaka)

   Tahap ini di lakukan dengan cara mengkaji dan mempelajari literatur dan referensi berupa naskah ilmiah seperti *jurnal* dan *paper*, buku tentang

konsep *Internet of Things* (IoT), konsep *machine learning*, serta cara kerja algoritma *Decision tree c4.5* dan algoritma lainnya sehingga dapat menunjang metodologi yang akan di terapkan pada penelitian ini.

3. Tahap Ketiga (Perancangan Sistem)

   Tahap ini merupakan tahap dimana menentukan spesifikasi perangkat keras, tipe sensor, dan bahasa pemprograman yang akan di dipakai untuk membangun sistem secara keseluruhan. Setelah itu, barulah kemudian sistem dibangun dengan mengimplementasikan algoritma *Decision tree c4.5* sebagai *Intrusion Detection System* (IDS) pada sisi koordinator.

4. Tahap Keempat (Pengujian)

   Setelah semua sistem selesai dikonfigurasi dan dibangun, selanjutnya dilakukan pengujian sesuai dengan batasan masalah dan beberapa parameter pengukuran yang telah di tetapkan, untuk mendapatkan hasil yang lebih maksimal.

5. Tahap Kelima (Analisa)

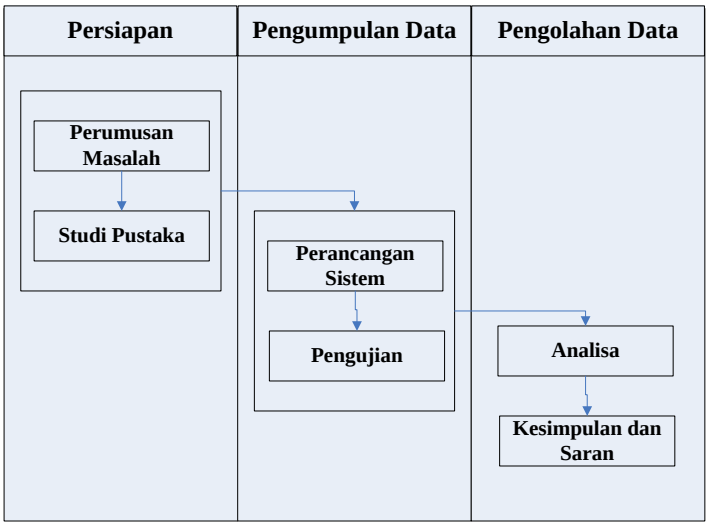
   Hasil dari pengujian pada tahap sebelumnya dilakukan analisa, dengan tujuan mengetahui kekurangan pada hasil perancangan dan faktor apa saja yang menjadi penyebabnya sehingga dapat di lakukan pengembangan pada penelitian selanjutnya.

6. Tahap Enam (Kesimpulan dan Saran)

   Pada tahap ini akan di lakukan penarikan kesimpulan berdasarkan studi pustaka, hasil perancangan sistem dan hasil dari analisa kerja sistem *Intrusion Detection System* (IDS) yang telah dibangun, dan beberapa poin saran dari penulis untuk penelitian selanjutnya.

Gambar 4.1 merupakan metodelogi yang digunakan dalam penyelesaian tugas ahir dengan judul “Pengenalan Pola Serangan *Denial of service* (DoS) pada Jaringan *Internet of things* (IoT) dengan *Clustering* menggunakan Algoritma *Decision tree c4.5*”.

Metodologi yang digunakan.



Gambar 1.1 Metodelogi Penelitian

1.7 Sistematika Penulisan

Penyusunan laporan tugas akhir terdiri dari beberapa bab agar pembahasan lebih sistematik dan spesifik dengan rincian antara lain sebagai berikut:

BAB I. PENDAHULUAN

Pada bab I berisikan penjelasan secara sistematis mengenai topik penelitian yang diambil meliputi latar belakang, tujuan, manfaat, rumusan masalah, batasan masalah, metodologi penulisan dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada bab II berisikan mengenai dasar teori dari penelitian terkait mengenai seragan *Denial of service*, DARPA *Dataset*, *Snort*, *Algoritma Decision tree c4.5*, *Internet of things*, *Intrusion Detection System*, yang berkaitan langsung dengan penelitian. Bab ini akan menjadi tinjauan atau landasan dalam menganalisis batasan masalah yang telah dikemukakan pada bab sebelumnya.

BAB III. METODOLOGI

Pada bab III berisikan tentang penjelasan secara bertahap mengenai proses penelitian yang dilakukan. Penjelasan tersebut meliputi tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV. PENGUJIAN DAN ANALISIS

Pada bab IV menjelaskan mengenai hasil dari pengujian (*experiment*) yang telah dilakukan selama penelitian tugas akhir. Hasil dari pengujian tersebut akan diklasifikasikan dengan menggunakan *Algoritma Decision tree c4.5*.

BAB V. KESIMPULAN DAN SARAN

Pada bab V berisi kesimpulan akhir dari pembahasan penelitian yang telah dilakukan. Pada bab ini juga terdapat saran-saran yang mungkin di perlukan dalam pengembangan penelitian selanjutnya dari pengujian dan analisis tugas ahir.

DAFTAR PUSTAKA

[1] A. Al-fuqaha, S. Member, M. Guizani, M. Mohammadi, and S. Member, "Internet of Things : A Survey on Enabling," vol. 17, no. 4, pp. 2347–2376, 2015.

[2] A. Zanella *et al.*, "Internet of Things for Smart Cities," vol. 1, no. 1, pp. 22–32, 2014.

[3] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things : A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[4] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-porisini, "Security , privacy and trust in Internet of Things : The road ahead," *Comput. NETWORKS*, vol. 76, pp. 146–164, 2015.

[5] M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues , Challenges , and Open Problems in the Internet of Things," 2015.

[6] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection : Methods , Systems and Tools," pp. 1–34, 2013.

[7] M. A. Ambusaidi, X. He, S. Member, P. Nanda, S. Member, and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," vol. 9340, no. NOVEMBER 2014, pp. 1–13, 2016.

[8] F. Iglesias and T. Zseby, "Analysis of network traffic features for anomaly detection," *Mach. Learn.*, no. December 2013, pp. 59–84, 2015.

[9] A. N. Riski Pristi Ananto, Yudha Purwanto, "Detection of attack on Distributed Denial Of Service based on Clustering and Classification using MINKOWSKI WEIGHTED K-MEANS Algorithm and DECISION TREE," vol. 4, no. 1, pp. 879–886, 2017.

[10] D. Farid, L. Zhang, C. Mofizur, M. A. Hossain, and R. Strachan, "Expert Systems with Applications Hybrid decision tree and naïve Bayes classifiers for multi-class classification tasks," *Expert Syst. Appl.*, vol. 41, no. 4, pp. 1937–1946, 2014.

[11] N. G. Relan and P. G. Student, "Implementation of Network Intrusion Detection System using Variant of Decision Tree Algorithm," pp. 3–7, 2015.

[12] A. Prabakar, R. Rajeswari, and R. Rajaram, "Procedia Engineering Network

Anomaly Detection by Cascading K-Means," vol. 30, no. 2011, pp. 174–182, 2012.

[13] P. M. Kumar and U. D. Gandhi, "machine learning algorithm for early detection of heart," *Comput. Electr. Eng.*, vol. 0, pp. 1–14, 2017.

[14] I. Y, E. A, I. A, and T. H, "I nternet of T hings A rchitecture : R ecent A dvances , T axonomy , R equirements , and O pen C hallenges," no. June, pp. 10–16, 2017.

[15] S. Niksefat, P. Kaghazgaran, and B. Sadeghiyan, "Privacy issues in intrusion detection systems : A taxonomy , survey and future directions," *Comput. Sci. Rev.*, pp. 1–10, 2017.

[16] S. Ji, B. Jeong, S. Choi, and D. Hyun, "Journal of Network and Computer Applications A multi-level intrusion detection method for abnormal network behaviors," *J. Netw. Comput. Appl.*, vol. 62, pp. 9–17, 2016.

[17] F. Montori, L. Bedogni, and L. Bononi, "A Collaborative Internet of Things Architecture for Smart Cities and Environmental Monitoring," vol. 4662, no. c, pp. 1–14, 2017.

[18] C. N.-C. N-, "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks," vol. 18, no. 1, pp. 110–113, 2014.

[19] M. Geva and A. Herzberg, "Bandwidth Distributed Denial of Service :," no. February, pp. 54–61, 2014.

[20] A. Singh and D. Juneja, "Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks," *Aarti Singh et. al. / Int. J. Eng. Sci. Technol.*, vol. Vol. 2(8), no. January, pp. 3405–11, 2016.

[21] A. Rghioui, A. Khannous, and M. Bouhorma, "Denial-of-Service attacks on 6LoWPAN-RPL networks : Threats and an intrusion detection system proposition," no. January, 2014.

[22] S. Sahu, "Network Intrusion Detection System Using J48 Decision Tree," pp. 2023–2026, 2015.

[23] A. F. Tyas and I. Atastina, "Klasifikasi Data Dengan Menggunakan Algoritma C4.5 Dan Tan (Tree Augmented) Naive Bayes," 2010.

[24] M. Kumar, "Intrusion Detection System Using Decision Tree Algorithm."

[25] J. Naik and S. Patel, “Tumor Detection and Classification using Decision Tree in Brain MRI,” vol. 14, no. 6, pp. 87–91, 2014.

[26] C. A. Oktavia and P. B. S, “Analisis Kinerja Algoritma C4.5 Pada Sistem Pendukung Keputusan Penentuan Jenis Pelatihan,” vol. 9, no. 2, pp. 144–149, 2015.

[27] Y. Mardi, “Jurnal Edik Informatika Data Mining : Klasifikasi Menggunakan Algoritma C4 . 5 Data mining merupakan bagian dari tahapan proses Knowledge Discovery in Database (KDD) . Jurnal Edik Informatika,” vol. V2.i2, no. ISSN : 2407-0491 E-ISSN : 2541-3716, pp. 213–219, 2013.

[28] Y. Mardiana and J. Sahputra, “Analisa Performansi Protokol TCP, UDP dan SCTP Pada Lalu Lintas Multimedia,” vol. 13, no. 2, pp. 73–84, 2017.

[29] A. K. Santra and C. J. Christy, “Genetic Algorithm and Confusion Matrix for Document Clustering 1,” vol. 9, no. 1, pp. 322–328, 2012.

[30] V. No, S. Sandra, and A. Heryanto, “Visualisasi Serangan Brute Force Menggunakan Metode K-Means dan Naïve Bayes,” vol. 2, no. 1, pp. 315–320, 2016.

[31] P. Rafiuddin Syam, *Seri Buku Ajar Dasar Dasar Teknik Sensor*. 2013.

[32] Y. Alif, K. Utama, and S. St, “Perbandingan Kualitas Antar Sensor Suhu dengan Menggunakan Arduino Pro Mini,” *e-Jurnal Nar. E-ISSN 2407-7712*, vol. 2, no. 2, p. 6, 2016.

[33] M. Yan, E. Adiptya, and H. Wibawanto, “Sistem Pengamatan Suhu dan Kelembaban Pada Rumah Berbasis Mikrokontroller ATmega8,” vol. 5, no. 1, pp. 15–17, 2013.

[34] S. Sensor, A. Asap, A. Tujuan, and S. Mq, “MQ 2 Sebagai Sensor Anti Asap Rokok ... (Mauludin dkk.),” pp. 260–265, 2016.

[35] M. F. Pradipta, S. Hardienata, and A. Chairunnas, “MODEL ALAT PENDETEKSI ASAP ROKOK MENGGUNAKAN SENSOR GAS MQ2 BERBASIS SMS GATEWAY.”