Terbit online pada laman web jurnal : **http://jurnal.iaii.or.id**

JURNAL RESTI

(Rekayasa Sistem dan Teknologi Informasi)

Vol. 2 No. 3 (2018) 685 – 696 ISSN : 2580-0760 (media online)

Implementasi Analisis NIDS Berbasis Snort Dengan Metode Fuzy Untuk Mengatasi Serangan LoRaWAN

Della Vinka Sandi[a], Muhammad Arrofiq[b]

[a]Departemen Teknik Elektro dan Informatika, Sekolah Vokasi, Universitas Gadjah Mada, sandivinka@gmail.com

[b]Departemen Teknik Elektro dan Informatika, Sekolah Vokasi, Universitas Gadjah Mada, rofiqm@gmail.com

Abstract

Indonesia is one of agrarian countris which has a fertile soil condition, but the agricultural products nowadays are not maximal in certain areas particularly strawberry plantation. Strawberry plant it self needs precise temperature and humidity level to maximize strawberry harvest. Soil humidity and air temperature are changing many times caused by the weather. Therefore, this research will build a prototype which is called Smart Agriculture for monitoring the temperature and soil humidity in strawberry plantation. Temperature and soil humidity data will be sent through wireless transmission media to smartphone using LoRa and LoRaWAN technology. This technology could send the data in a long distance but it's server is vulnerable to attacks such as flooding payload data from LoRa node, ping of death or ping flooding, and scanning port. This research implements that attack on LoRaWAN network server which influences server bandwidth , delay, jitter, and throughput from normal condition. To detect an attack, Snort NIDS method and attack classification are used with fuzzy logic method. The result of this research are temperature and humidity readings, attack notification, and attacker address blocking. Besides, it has proven that fuzzy and snort can optimize server performance.

Keywords: Smart Agriculture, LoRa, LoRaWAN, Snort, NIDS, Fuzzy

Abstrak

Indonesia merupakan salah satu negara agraris dengan kondisi tanah yang sangat subur, tetapi perlu diketahui bahwa hasil dari pertanian saat ini belum maksimal di beberapa daerah, seperti halnya pada perkebunan stroberi. Tanaman stroberi sendiri membutuhkan tingkat suhu dan kelembaban udara yang tepat, agar hasil panen stroberi lebih maksimal. Kelembaban tanah dan suhu udara sering kali berubah tergantung cuaca, untuk itu penelitian ini akan membuat suatu alat atau portotipe yang disebut *Smart Agriculture* untuk melakukan monitoring suhu dan kelembaban tanah pada perkebunan stroberi. Data suhu dan kelembaban tanah akan dikirimkan melalui media *transmisi nirkabel* menuju ke *smartphone* menggunakan LoRa dan teknologi LoRaWAN. Teknologi ini mampu mengirimkan data dalam jarak yang cukup jauh, namun *server* rentan terhadap serangan seperti *flooding payload data* dari *LoRa node*, *ping flooding* dan *scanning port*. Pada penelitian ini menerapkan serangan itu pada LoRaWAN *network server* yang berpengaruh pada *Bandwidth*, *Delay*, *Jitter* dan *Throughput* dari kondisi normal. Untuk melakukan deteksi serangan diimplementasikan metode *Snort NIDS* dan pengelompokan tindakan serangan (*low*, *medium*, *high*) dengan metode *fuzzy logic*. Hasil dari penelitian ini adalah berupa tindakan berupa pembacaan suhu dan kelembaban, notifikasi serangan dan blok alamat *attacker*. Selain itu dapat dibuktikan bahwa dengan adanya fuzzy dan snort mampu mengoptimalkan performa server.

Kata Kunci : *Smart Agriculture*, LoRa, LoRaWAN, *Snort*, NIDS, *Fuzzy*

1. Pendahuluan

Internet of Things yang sering dikenal juga dengan singkatan IoT, merupakan konsep yang menghubungkan seluruh aktivitas pada suatu konektivitas internet dan bersifat *real time* (terus menerus). *IoT* saat ini sedang berkembang di Indonesia yang diharapkan mampu untuk mengatasi berbagai permasalahan di semua bidang termasuk juga dalam bidang pertanian dan perkebunan. Keadaan di Indonesia yang saat ini memiliki iklim dan curah hujan yang mulai tidak menentu. Dengan kondisi tersebut, membuat para petani sering mengalami kerugian atau kegagalan panen. Salah satu faktor terbesar dalam perkebunan adalah masalah pengaturan kelembaban tanah. Kelembaban tanah dapat mempengaruhi kehidupan biologi di dalam tanah dengan kelembaban tanah yang tinggi dapat juga meningkatkan serangan penyakit tanaman.

Permasalahan terkait pengontrolan kelembaban tanah sering terjadi juga di perkebunan stroberi. Dari

Diterima Redaksi : 23-07-2018 | Selesai Revisi : 19-12-2018 | Diterbitkan Online : 15-12-2018

berbagai permasalah tersebut menjadikan suatu dorongan bagi para peneliti untuk memberikan solusi dalam beragam model dan metode analisis (Dr. Aqeel, 2017). Salah satunya mengembangkan sistem yang mampu mengatasi hal tersebut dengan menggunakan teknologi IoT dengan istilah *Smart Agriculture*. Dalam sistem IoT pada *Smart Agriculture* ini memiliki alur data dari *controller*, *server*, ataupun perangkat lain yang terhubung seperti perangkat *mobile*. Pengiriman data dari sensor dengan menggunakan teknologi LoRa merupakan teknologi yang saat ini tengah berkembang di dunia IoT. Dengan jarak antara *node sensor* dan *gateway* bisa mencapai 15 Km. Selain itu dengan LoRa , dapat diterakan Topologi *Star* yang mampu menghemat biaya untuk perangkat. Dengan satu *gateway* dapat digunakan untuk beberapa *node sensor* dalam pengiriman datanya.

Data yang dikirimkan akan dilewatkan pada network server pada lora disebut sebagai lorawan *network server*. Pada *server* tersebut dimungkinkan adanya beberapa serangan yang dapat mengakibatkan kenaikan dari Bandwidth, delay, jitter dan throughput. Pada penilitian ini penulis akan mengimplementasikan *Snort* IDS pada lorawan *network server* untuk monitoring trafik jaringan dan menggabungkan dengan metode fuzzy didalamnya. Metode *Fuzzy logic* yang digunakan pada penelitian ini berdasarkan data dari *database* S*nort* dengan metode *fuzzy* sugeno. Dan akan dikelompokan kedalam empat tingkatan tindakan yaitu very low, low, *medium*, dan *high* dari serangan terhadap LoRaWAN *network server*. Serangan yang akan dilakukan uji berupa serangan *flooding payload* data, *flooding ping* atau ICMP, dan *scanning port*. Penerapan metode *fuzzy logic* juga dapat menentukan *inline mode* dari *snort*, apakah paket data dari sumber tersebut diperbolehkan atau *allow* paket atau akan dilakukan *drop* sesuai durasi waktu dari hasil defuzzyfikasi.

Dalam penelitian ini, diangkat suatu rumusan masalah mengenai perancangan fuzzy pada Snort NIDS agar dapat melakukan tindakan pencegahan yang sesuai dengan kategori dan frekuensi serangan yang diberikan. Adapaun batasan masalah yang terdapat pada penelitian ini adalah (a) Metode *fuzzy logic* diterapkan untuk menentukan keputusan dari tindakan dari data *snort* NIDS dengan membagi kedalam empat tindakan yaitu very low, *low attack*, *medium attack* dan *high attack* berupa tindakan *blok* terhadap *source address attacker* dan mengirimkan notifikasi serangan pada android.

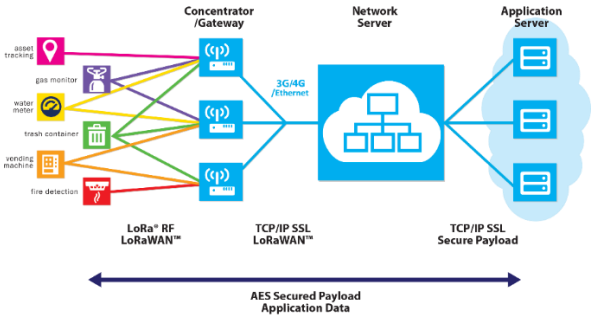
2. Tinjauan Pustaka

Berdasarkan latar belakang permasalahan terkait dengan serangan LoRaWAN Network Server pada smart Agriculture, dilakukan beberapa tinjauan pada pustaka terkait mengenai penerapan teknologi LoRaWAN, implementasi Snort NIDS dan Metode fuzzy sebagai komponen utama dalam penelitan ini.

2.1 Long Range Wide Area Network (LoRaWAN)

Teknologi Lora dikembangkan oleh perusahaan Perancis bernama Cycelo, yang setelah itu diakuisisi oleh Semtech pada tahun 2012. *Long Range* (LoRa) merupakan lapisan fisik apabila disandingkan dengan OSI layer. Frekuensi LoRa berada dibawah 1 GHz, di negara Eropa dirancang untuk menggunakan frekuensi diatas 433 / 868 MHz, sementara di bagian Amerika Serikat menggunakan lebih dari band 915 MHz, menurut "*IoT augmented with STM32 MCUs & LoRa*" (Andrei, Radoi & Tudose, 2017) .

LoRaWAN menerapkan topologi star on star untuk menyampaikan pesan ke *server* pusat melalui *gateway*. Tujuan untuk menggunakan topologi *star* yaitu mempertahankan daya baterai sekaligus untuk meningkatkan jangkauan komunikasi. Setiap *end node* mentrasmisikan data ke *gateway*. *Gateway* yang akan meneruskan data ke *server* jaringan. Saat transmisi inilah dilakukan pendeteksian redudansi, keamanan, dan penjadwalan untuk pengiriman pesa. Selain itu dengan menggunakan topologi seperti gambar 1 maka akan memudahkan untuk melakukan pelacakan perangkat, karena *end node* mampu berkomunikasi ke beberapa *gateway* tanpa adanya kebutuhan untuk komunikasi *gateway to gateway.* Dengan adanya *server* yang terpusat juga dapat mengurangi masalah adanya *collision.*



Gambar 1. Arsitekur LoRaWAN

Long Range Wide Area Network (LoRaWAN) merupakan evolusi dari jaringan sensor *nirkabel* yang diarahkan ke konsep *Internet of Things*, yang memerlukan konektivitas dari sensor ke internet. Teknologi LoRa merupakan solusi yang mampu mengatasi masalah dari konsep IoT. LoRaWAN memiliki potensi sangat besar karena cocok untuk berbagai aplikasi IoT Sehingga muncullah beberapa penelitian terkait teknologi LoRa. Dengan mempelajari berbagai potensi LoRa dan LoRaWAN sehingga peneliti mampu menemukan kekuatan atau kelebihan dan keterbatasan dari LoRa.

Penelitan pengujian terhadap kemampuan Lora telah dilakukan sebelumnya, peneelitian tersebut memiliki hasil bahwa dengan LoRa mampu mencapai jarak 4,3 Km di daerah perkotaan dan jarak 9,7 Km diatas lapangan terbuka luar kota. Sehingga dari pengujian ini tidaklah menjadi masalah terhadap jangkauan

protokol LoRa. Dari penelitian tersebut dapat disimpulkan bahwa LoRa dan LoRaWAN menjadi media komunikasi yang hebat untuk aplikasi yang tidak memerlukan data *real time* atau *high resolution*. Seperti halnya, dalam pemanfaat untuk memantau kelembaban tanah di bidang pertanian. (Andrei, Radoi & Tudose, 2017) Protokol LoRa diproduksi oleh *Microchip* yang saat ini sangat bagus untuk interkoneksi perangkat melaui internet. Komunikasi Internet sangatlah rentan dengan adanya permasalahan terkait dengan keamanan.

2.2 Keamanan Jaringan

Keamanan jaringan saat ini menjadi permasalahan yang penting dalam teknologi komputer, sebelumnya telah terdapat beberapa penelitian yang mengarah pada keamanan data. Serangan yang mengancam keamanan pada jaringan bisa juga melalui beberapa celah seperti port komunikasi untuk dimasuki secara illegal. Penelitian yang dilakukan oleh Irwan Sembiring, dkk pada tahun 2009, telah melakukan penelitian bahwa celah port komunikasi sehingga peneliti menerapkan port knocking yang mampu melakukan komunikasi melalui port yang tertutup. Dengan implementasi menggunakan dua buah komputer yang saling terhubung, komputer A berfungsi sebagai port knocking dan komputer B sebgai klien yang meneruskan data ke server dengan menguji port SSH. Dan hasil penelitian tersebut metode port knocking dan firewall mampu diiimplementasikan pada jaringan yang tidak terlalu padat, karena pada jalur lalu lintas jaringan padat port harus terbuka dan dapat diakses secara terus menerus.

Keamanan jaringan dapat rentan kaitannya dengan aplikasi dan layanan yang berjalan pada perangkat, seperti halnya port yang aktif dan tidak aktif. Tetapi selain itu, kemanan jaringan juga dibutuhkan pada jaringan nirkabel. Biasanya seorang attacker akan melakukan penyerangan pada server penyedia hotspot ataupun penggunanya. Penelitian telah dilakukan sebelumnya oleh Mustofa dan Ariwibowo pada tahun 2013. Penelitian tersebut menerapkan kombinasi antara honeypot honeyd sebagai keamanan jaringan hotpsot dan IDS untuk mendeteksi adanya serangan yang ditujukan ke jaringan hotspot. Honeypot akan melakukan rekaman aktifitas dari penyerang terhdap server palsu yang memberikan layanan mirip dengan server utama. Hasil dari penelitian ini, kombinasi yang dihasilkan dari honey pot dan Intrusion Detection Syste (IDS) dengan Honeyd dan Snort dapat memberikan keamanan berlapis dengan menipu dan deteksi serangan.

2.3 Snort *Network Intrusion Detection System*

Intrusion Detection System (IDS) adalah aplikasi perangkat lunak atau perangkat keras yang mampu melakukan deteksi aktifitas yang mencurigakan dalam suatu jaringan. IDS mampu melakukan inspeksi pada lalu lintas inbound dan outbound, melakukan analisa, dan mencari bukti dari percobaan intusion (Jannah, dkk, 2009). IDS dapat didefinisikan sebagai tools, metode atau resource yang memberikan bantuan untuk identifikasi, pemberian laporan terhadap aktifitas jaringan. IDS dikenal sebagai monitoring suatu jaringan. Dengan adanya monitoring, kejadian mencurigakan akan dapat diketahui lebih awal oleh admin dan melakukan pencegahan dari segala kemungkinkan yang bisa terjadi.

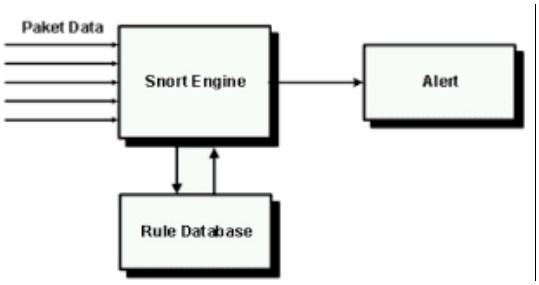
Snort merupakan salah contoh program dari *Network-based Intrusion Detection System*. Merupakan program yang dapat mendeteksi tindakan atau aktifitas penyusupan pada jaringan komputer. *Snort* bersifat *open source* dengan lisensi GNU *General Purpose License* sehingga dapat digunakan untuk mengamankan sistem server tanpa biaya lisensi (Snort team 2009). *Snort* dapat dikonfigurasi dan dijalankan untuk periode lama tanpa pengawasan dan perawatan bersifat *administrative*. Karena *snort* merupakan sistem keamanan terpadu dalam jaringan. *Snort* dapat berjalan pada semua platform dimana libpcap dapat bejalan. Sistem operasi tersebut yang telah diuji adalah RedHat Linux, Debian Linux, MkLinux, HP-UX, Solaris, x86 Free/Net/OpenBSD. Windows dan MacOS X.

Snort sebagai IDS dalam jaringan dapat dilakukan dengan tiga konsep penempatan atau Snort IDS Placement yang berbeda sebagai berikut :

a. Snort Network Intrusion Detection System
   Snort NIDS tidak hanya melakukan monitoring paket data pada perangkat jaringan mesin Snort, tetapi juga terhadap seluruh trafik jaringan di satu segmen jaringan dalam snort berada.
b. Snort Host-Base Intrusion Detection System
   Snort HIDS melakukan pengamatan trafik data pada perangkat jadingan dimana aplikasi Snort IDS ditempatkan. Biasanya snort akan dijalankan pada mesin dengan aplikasi layanan lain seperti web server, ITP server maupun SQL server.
c. Snort Distibuted Intrusion Detection System
   Konsep ini menggunakan perpaduan dari konsep Network IDS dan Host-Based IDS. Masing – masing diletakkan pada bagian dalam segmen jaringan yang dikendalikan oleh sebuah mesin yang digunakan sebagai pusat manajemen sistem keamanan terpusat. Pusat manajemen IDS akan menentukan rule yang digunakan oleh setiap sensor IDS dan mengumpulkan hasil peringatan dari tiap sensor dalam jaringan melalui sistem database terpusat. Untuk menentukan penggunaan NIDS atau HIDS sesuai dengan kebutuhan.

Snort IDS mempunyai tiga komponen utama yang saling berhubungan satu sama lain. Pada gambar 4.14 dibawah adalah skema dari komponen yang terdiri dari snort engine, rule snort, dan alert. Snort engine adalah program sebagai daemon proses yang berkerja untuk membaca paket dan membandingkan dengan

rule Snort. Rule Snort merupakan database yang berisi pola – pola serangan yang berupa signature jenis serangat. Rule ini harus sering dilakukan update sehingga dapat mengenali serangan yang baru yang akan dikirimkan dalam bentuk peringatan atau alert. Alert merupakan catatan atau peringatan dari pendeteksian Snort.



Gambar 2. Skema komponen Snort NIDS

2.4 Metode Logika Fuzzy

Logika *fuzzy* pertama kali dikembangkan oleh Lotfi A. Zadeh pada tahun 1965 tentang teori himpunan fuzzy. Logika *fuzzy* sudah diterapkan pada banyak bidang, mulai dari teori kendali hingga inteligensia buatan. Logika fuzzy diterapkan pada masalah – masalah yang mengandung unsur ketidakpastian (*uncertainty*), ketidaktepatan *(imprecide*), *noisy* dan sebagainya. Komponen pada sistem *fuzzy* yaitu variabel *fuzzy*, himpunan *fuzzy*, semesta pembicaraan dan domain (Rinaldi Munir, 2005). Adapun tahapan dari logika fuzzy sebagai berikut :

1. Penentuan Variabel dan Domain

Penentuan Variabel yang akan dibahas dalam sistem fuzzy, contohnya : umur, temperature, permintaan, dan lainnya. Sedangkan himpunan fuzzy meruapakan suatu grup yang mewakili kondisi tertentu dalam suatu variabel fuzzy. Conrohnya variabel umur yang terbagi menjadi 3 himpunan fuzzy, yaitu : Muda, Parubaya, dan Tua. Setelah itu menentukan Domain himpunan fuzzy yang merupakan batasan nilai yang diijinkan untuk beroperasi.

2. Fungsi Keangotaan dan Fuzzyfikasi

Menurut Kusumadewi dan Purnomo (2010) fungsi keanggotaan (membership function) adalah suatu kurva yang menunjukkan pemetaan titik-titik input data kedalam nilai keanggotaannya (sering juga disebut dengan derajat keanggotaan) yang memiliki interval antara 0 sampai 1. Salah satu cara yang dapat digunakan untuk mendapatkan nilai keanggotaan adalah dengan melalui pendekatan fungsi. Fungsi – fungsi akan direpresentasikan dalam bentuk kurva seperta kurva linear, segitiga, trapezium dan lain – lain. Kali ini akan dibahas representasi dalam bentuk kurva segitiga

3. Rule Evaluation

Evaluasi aturan merupakan proses pengambilan keputusan (inference) yang berdasarkan aturan - aturan yang ditetapkan pada basis aturan (rules base) untuk menghubungkan antar peubah-peubah fuzzy masukan dan peubah fuzzy keluaran. Aturan - aturan ini berbentuk jika ... maka (IF ... THEN). Pada tahap ini, hasil dari fuzzifikasi pada setiap rule akan dilihat kembali. Secara sintaks, suatu fuzzy rule (aturan fuzzy) dituliskan sebagai:

– IF antecendent THEN consequent

4. Defuzzyfikasi

Defuzzyfikasi merupakan kebalikan dari fuzzyfikasi, yaitu pemetaan dari himpunan fuzzy ke himpunan tegas.Input dari proses defuzzyfikasi adalah suatu himpunan fuzzy yang diperoleh dari komposisi aturanaturan fuzzy. Hasil dari defuzyfikasi ini merupakan output dari sistem kendali logika fuzzy. Pada proses defuzzifikasi akan menghasilkan nilai z. Dimana z memiliki persamaan sebagai berikut :

$$Z= \frac{\alpha pred1 * z1 + \alpha pred2 * z1 + \alpha pred3 * z(1) + \ldots + \alpha pred\ (n) * z(n)}{\alpha pred1 + \alpha pred2 + \alpha pred3 + \ldots + \alpha pred\ (n)}$$

3. Metodologi Penelitian

Tahapan penelitian yang dilakukan dalm proyek akhir ini pertama yaitu studi literatur dari beberapa jurnal dan buku, melakukan perancangan dan analisa sistem kebutuhan. Melakukan persiapan untuk perangkat keras yang dibutuhkan dan perangkat lunak. Dilanjutkan dengan melakukan konfigurasi pada lora *client* , konfigurasi gateway, konfigurasi pada lora *network server*, konfigurasi *application server*. Apabila lorawan berhasil maka dilanjutkan dengan proses instalasi Snort NIDS pada lorawan network server dan menambahkan rule pada database untuk melakukan alert dan tindakan terhadap serangan. Melakukan sniffing paket dan lalu lintas jaringan, yang selanjutnya menyimpan log snort pada database. Data pada log snort akan dilakukan proses pengelompokan tindakan berdasarkan metode Fuzzy *Flowchart* pada gambar 3.1 berikut ini menunjukkan metode penelitian yang dilakukan oleh penulis

3.1 Alat dan Bahan

Proses implementasi dan analisa network intrusion detection system berbasis snort dengan metode fuzzy untuk mengatasi serangan menggunakan lorawan pada smart agriculture memerlukan alat dan bahan sebagai berikut.

1. Perangkat Keras
   a. 3 Arduino Uno
   b. 3 LoRa Shield frekuensi 915 Mhz
   c. 1 Dragino LoRa Gateway
   d. 2 Raspberry Pi 3 Model B

Tabel 1. Spesifikasi Raspberry Pi

Sistem Operasi	Memori	Daya
Rasbian Jessie	32 GB	2 A

e. 2 Sensor Kelembaban Tanah *YL-69*
f. 2 Sensor Suhu DHT11
g. 1 PC / Laptop Application Server

Tabel 2. Spesifikasi Laptop App Server

Sistem Operasi	Memori	CPU	Harddisk
Windows 10	2 GB	2,00 GHz	500 GB

h. 1 PC / Laptop Mesin Penyerang
i. 1 Smartphone Client

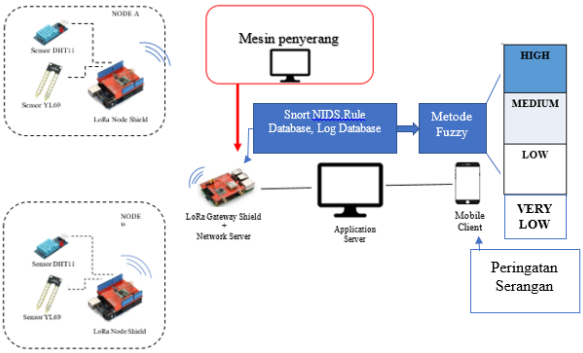
3 Perangkat Lunak
a. Arduino IDE
b. Raspbian Jessie
c. Windows 10
d. Mosquitto Server (broker)
e. Postgresql
f. MySQL
g. Snort, Libpcap, libdnet, daq, adodb
h. Nmap
i. PingFlood
j. SQLMap
k. Python
l. Android Studio

3.2 Implementasi Sistem Pengujian

Infrastruktur yang digunakan pada proyek akhir ini dirancang dalam tiga buah skenario sebagai berikut. Pada skenario pertama terdiri dari 2 arduino uno yang terhubung dengan lora *shield* dragino *client*, 1 raspberry pi 3 model B yang terhubung dengan LoRa GPS HAT sebagai *gateway* dan LoRa *network server*, 1 PC sebagai LoRa *application server*, dan 3 *smartphone client*. Metode fuzzy diimplementasikan untuk penentuan tindakan dan peringatan berdasarkan data snort. Skenario ini berfungsi untuk mengetahui apakah metode fuzzy dapat mengoptimalkan kinerja dari Snort NIDS dalam melakukan pencegahan terhadap adanya aktifitas mencurigakan, dan menentukan tindakan dari serangan berupa alert yang akan dikirim ke admin dan time waktu tertentu untuk melakukan blok terhadap source address attacker, pada gambar 3 merupakan topologi dari skenario pengujian.

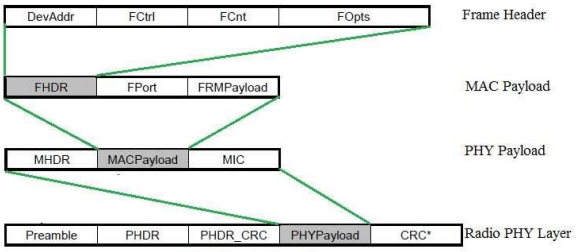
3.3 Pembacaan dan Pengiriman Data LoRaWAN

Data pada penelitian ini berasal dari data pembacaan sensor DHT11 dan sensor YL69. Dalam pengiriman data menuju aplikasi android menggunakan LoRaWAN. Dengan menggunakan LoRa Dragino Shield dan LoRa GPS Hat Gateway. Proses pengiriman data sensor data akan diubah terlebih dahulu menjadi suatu paket data LoRaWAN.



Gambar 3. Skenario Penelitian

Paket data atau biasa disebut dengan format data pada LoRa terdiri dari preamble, physical header (PHDR) , Physical header CRC, Physical payload. Pada blok physical payload berisikan suatu frame payload. Sebelum payload dikirimkan akan ditambahkan terlebih daulu dengan Frame Header yang berisikan device address, frame control, frame counter, frame opts. Dari frame header yang terbentuk akan ditambahkan frame port dan frame payload (data sensor) yang disebut dengan MAC payload. Kemudian MAC payload akan ditambahkan MAC header dan MIC yang siap untuk dikirimkan dalam bentuk physical payload. Pada gambar 4 dibawah menggambarkan format dari pesan LoRaWAN tiap sesinya., dimana data yang dikirimkan berada pada sesi paling bawah yaitu radio physical layer. Seluruh data yang dikirimkan akan dienkripsi dengan AES128 dan encode base64



Gambar 4. Format Pesan LoRaWAN

3.4 Proses Serangan LoRaWAN Server

Serangan pada penelitian ini terdiri dari tiga serangan yaitu Ping Flooding, Data Flooding, dan Port Scanning. Dari ketiga serangan tersebut diidentifikasi atau dikelompokkan menjadi tiga tingkatan serangan yaitu Low, Medium dan High. Dengan ketentuan tingkatan seperti pada tabel 3. Ping flooding dikelompokkan berdasarkan besarnya byte yang dikirimkan, data flooding berdasarkan data UDP packet dengan besaran data sesuai tabel. Sedangkan pada port scanning tergantung jenis scanning yang digunakan yang berkaitan dengan berapa jumlah port yang di scanning. Dari tingkatan low medium dan high memiliki nilai priority yang akan dikelompokkan

pada himpunan fuzzy berdasarkan serangan sub bab berikutnya.

Tabel 3. Pengelompokan Serangan

Pengelom-pokan	Low	Medium	High
Ping Flooding	< 32 byte	32 byte – 64 byte	>64 byte
Data Flooding	< 32 byte	32 byte – 100 byte	>100 byte
Port Scanning	< 10 port	10 – 100 port	>100 port

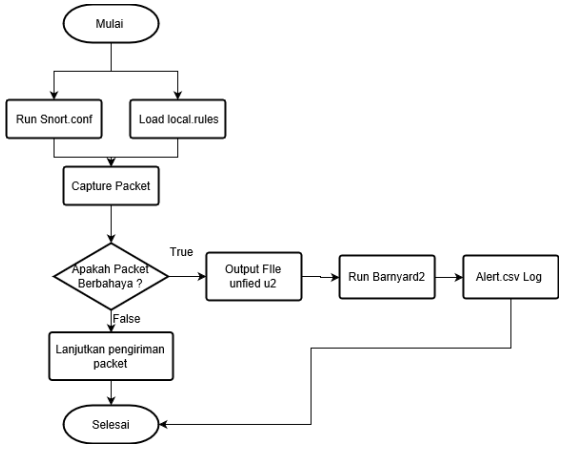
3.5 Proses Identifikasi Snort

Pada penelitian ini snort akan diinstall pada raspberry LoRaWAN network server. Untuk menjalankan snort menggunakan perintah berikut .

```
pi@raspberrypi:~ $ sudo snort -D -c /etc/snort/snort.conf -i wlan0
Spawning daemon child...
My daemon child 3030 lives...
Daemon parent exiting (0)
```

Gambar 5. Perintah Menjalankan Snort

Setelah perintah tersebut dijalankan maka akan mencocokkan dengan local.rules. apakah packet tersebut termasuk packet yang berbahaya atau bukan. Jika bukan maka packet akan langusng dikirimkan menuju application server. Tetapi apabila teridentifikasi sebagai suatu serangan, maka akan muncul suatu notifikasi dari snort dan tiap log sari snort akan disimpan dalam bentuk file unfied pada /var/log/snort. Pada penelitian ini menggunakan tools barnyard2 untuk mempermudah dalam konversi output. Sehingga saat menjalankan snort juga menjalankan barnyard2 sehingga tiap satu file log dari unfied akan langusng dikonversikan dalam bentuk output file dengan nama alert.csv. Pada gambar 6 merupakan gambar flowchart dari proses deteksi dengan snort.

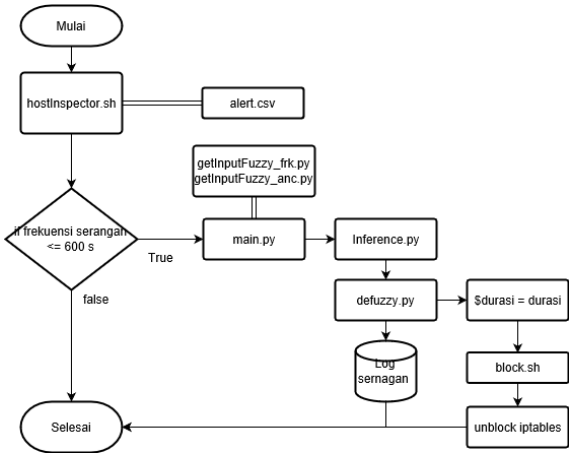


Gambar 6. Flowchart Penelitian

3.6 Proses Algoritma Fuzzy

Logika fuzzy diterapkan pada masalah – masalah yang mengandung unsur ketidakpastian (*uncertainty*), ketidaktepatan *(imprecide*), *noisy* dan sebagainya. Pada penelitian ini algoritma fuzzy digunakan sebagai pemberi keputusan untuk lama waktu atau durasi block iptables source address yang melalui LoRaWAN Network Server. Implementasi algoritma fuzzy diambil datanya dari alert.csv, yang dipanggil bersamaan dengan hostInspector.sh. File script hostInspector.sh digunakan sebagai inspector untuk melihat semua lalu lintas jaringan yang masuk pada LoRaWAN server. Setelah itu pada file hostInpector juga melakukan pengecekan apakah frekuensi serangan lebih dari 600 detik, apabila iya maka akan mengaktifkan fuzzy, tetapi apabila tidak maka dianggap sebagai bukan serangan dan melanjutkan aktifitas berikutnya.

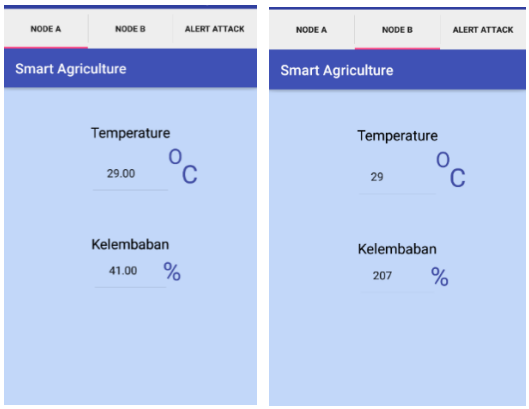
Pada gambar 7 berikut merupakan flowchart dari proses penentuan dan perhitungan dari algoritma fuzzy.



Gambari 7. Flowchat Proses Fuzzy

4. Hasil dan Pembahasan

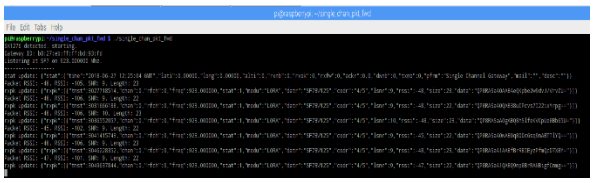
Pada bab ini akan menjelaskan mengenai proses pengiriman data LoRaWAN dan hasilnya, selain itu juga menjelaskan proses dari keamanan pada LoRaServer menggunakan Snort dengan metode Fuzzy beserta hasil yang telah dilakukan pada penelitian ini. Pembahasan pertama mengenai proses pengiriman data LoRaWAN yaitu data pembacaan sensor dari LoRa Node Shield yang dikirimkan menuju Android melalui gateway, LoRa Server, Application Server. Pengujian ini digunakan untuk melakukan pengecekan bahwa seluruh konfigurasi telah berjalan sehingga data dapat dibaca pada aplikasi android. Seperti pada gambar 8 berikut.



(a) (b)

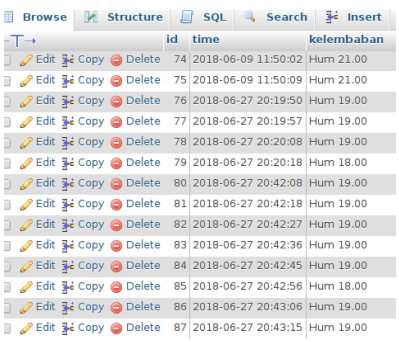
Gambar 8. Hasil Pembacaan Sensor Android Node A (a) dan Node B (b)

Setelah dari LoRa Shield akan dikirim pada gateway dilakukan proses enkripsi AES 128 dan encode data base64. Seperti pada gambar 9 yang merupakan hasil saat melewati gateway.



Gambar 9. Data Melalui Gateway LoRaWAN Packet Forwader

Data yang telah melewati gateway akan di publish oleh LoRa network Server menuju Application server menggunakan protocol MQTT dengan topic application/2/device/#. Pada application server terdapat subscriber untuk menerima data dari LoRaWAN Network server, dititik ini data dilakukan proses decode64 dan dimasukkan kedalam database sesuai dengan tabel suhu dan kelembabannya. Proses insert pada database dilakukan dengan menggambil karakter dari hasil decode, apabila data tersebut temp maka akan masuk pada suhu, sedangkan data tersebut kelembaban maka akan masuk pada tabel kelembaban. Data dari sensor akan disimpan dalam bentuk MySQL database dengan nama database smart dan terdapat dua tabel seperti pada gambar 10. Pada gambar tersebut data suhu yang dibaca pada LoRa Shield akan tersimpan sesuai di database.



Gambar 10. Hasil Data Akhir Pada Database Server

Selain digunakan untuk membuktikan konfigurasi LoRaWAN juga berfungsi untuk mengecek bandwidth , delay, jitter dan throughput pada LoRaWAN dengan satu node yang nantinya akan digunakan sebagai pembanding pengujian kedua terkait adanya serangan LoRaWAN Server. Pada tabel 4 merupakan hasil dari simulasi pengujian sebanyak 6 kali percobaan dengan satu kali percobaan selama satu menit.

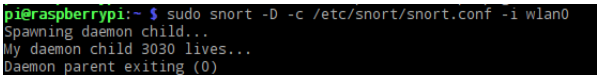
Tabel 4 Pengujian Performa Sebelum Serangan

ke-	Bandwidth TX (kbps)	Bandwidth RX (kbps)	Delay (seconds)	Jitter (seconds)	Througput Bit/sec
1	0,82	0,17	0,011753	0.0000096	1308
2	1,01	0,23	0,011234	0.0000717	1817
3	0,96	0.17	0,013092	0,0018658	1390
4	1.02	0.19	0,010865	0,0006032	1400
5	0.85	0,19	0,01326	0.0000096	1438
6	1.06	0.21	0,010756	0.0000375	1484
Rata 2	0.95	0.195	0,011827	0,000389	1473

Pada bagian berisi penjelasan ilmiah dari hasil penerapan metode penelitian yang telah ditetapkan pada sub bab 3.

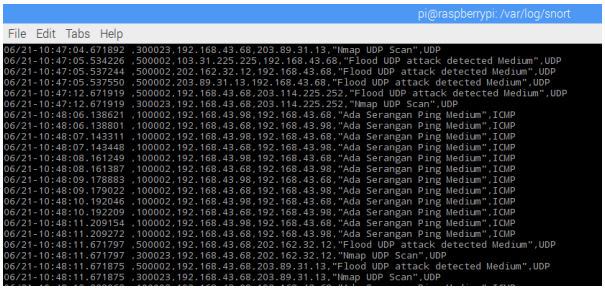
4.1 Proses Deteksi Serangan

Proses deteksi serangan menggunakan snort terdiri dari 2 tahap yaitu tahap pembacaan lalu lintas jaringan yang masuk , dan tahap log serangan dengan istilah snort output. Pada tahap pertama yaitu pembacaan lalu lintas menggunakan perintah seperti pada gambar 11 dibawah ini, dengan mengambil data dari konfigurasi snort dan disamakan apakah lalu lintas jaringan yang masuk merupakan salah satu serangan.



Gambar 11. Menjalankan Snort

Data yang dideteksi oleh snort pada penelitian ini dikonversikan kedalam file .csv sehingga hasil simulasinya seperti pada gambar 12. Pada gambar tersebut menunjukkan hasil dari output file.csv menggunakan snort.



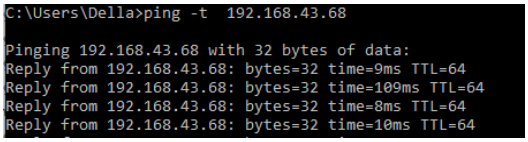
Gambar 12 Output File Alert.csv

4.2 Hasil Keterbuktian Snort

Pada pengujian kedua disimulasikan sesuai pada skenario kedua. Pada LoRaWAN network server apakah dapat diserang oleh ketiga serangan yang ditentukan yaitu ping flooding, data flooding dan scanning port. Selain ini pengujian kedua akan dapat dilakukan analisa apakah serangan mampu mempengaruhi kinerja dari LoRaWAN. Sehingga dalam sub bab ini akan dikelompokkan ke dalam tiap pengujian serangan sehingga terbentuk suatu data output dari snort yang ada pada file alert.csv

4.3 Serangan Ping Flooding

Serangan ping flooding menggunakan perintah ping dari command prompt yang pada penelitian ini menggunakan OS Windows 10. Terdapat tiga perintah yang berbeda. Perintah pertama yaitu ping dengan besaran data 32 byte seperti pada gambar 13 berikut.



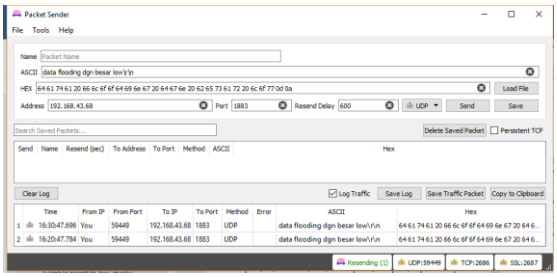
Gambar 13. Perintah Ping Flooding Low

Perintah kedua dengan besaran data 33 byte sampai dengan kurang dari 64 byte, dan perintah ketiga dengan besaran > 64000 byte. Untuk perintah ping pada serangan medium dan high seperti pada gambar 13 tetapi pada command –l disesuaikan dengan besarnya paket.

4.4 Serangan Data Flooding

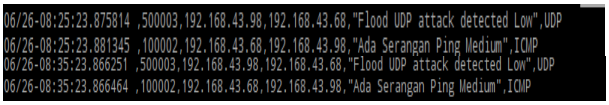
Serangan data flooding dilakukan menggunakan tools packet sender dengan variasi dari besarnya data. Pada penelitian ini untuk melakukan percobaan dilakukan generate data sebelumnya dengan tiga variasi besar data yang berbeda. Yaitu <32 byte sebagai uji coba serangan low, besar data 32 byte hingga 500 byte sebagai serangan medium dan besar data > 500 byte sebagai serangan high.

Pada penelitian ini untuk membuktikan dari keberhasilan snort pada jenis serangan data flooding UDP dengan melakukan uji coba sebanyak 24 kali dengan variasi besar data dan interval waktu yang berbeda beda. Uji coba pertama dilakukan dengan interval waktu 600 second dengan besar data 29 bytes dengan perintah dalam mesin penyerang seperti pada gambar 14 berikut. Pada packet sender tersebut ditunjukkan resend delay selama 600 dengan menggunakan port 1883 dan UDP, Address 192.168.43.64 merupakan alamat IP dari LoRa Network Server. Pada percobaan ini terdapat dua data yang dikirimkan pada waktu 16.20.47.784 dan pengiriman kedua pada waktu 16.30.47.696,kedua data tersebut yang akan dilakukan analisa pada penelitian ini.



Gambar 14 Flooding Data Low Dengan Delay 600 s

Serangan yang dikirimkan dari mesin penyerang akan diidentifikasi oleh snort dan memberikan output notifikasi yang dimasukkan dalam file alert.csv seperti pada gambar 15 berikut dengan identifikasi sebagai serangan low.



Gambar 15 Output File Alert.csv Low Dengan Delay 600 s

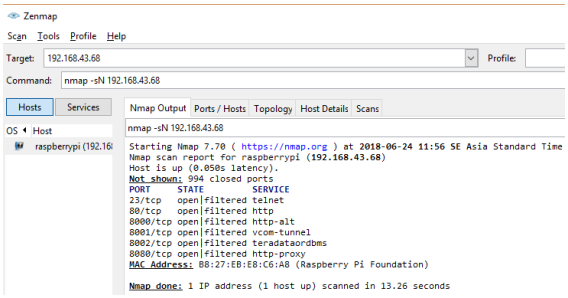
Untuk serangan data flooding percobaan berikutnya sama seperti pada perintah gambar … dengan merubah load file data yang low medium atau high. Dan menvariasi resend delay dari 600 menjadi 540, 360.10, dan 6 detik.

4.5 Serangan Port Scanning

Serangan yang dilakukan pada penelitian ini selanjutnya adalah serangan port scanning menggunakan tools NMap. Variasi serangan NMap ditentukan berdasarkan seberapa besar scanning yang dilakukan hall scan atau full scan port. Pada percobaan ini untuk membuktikan keberahasilan dari snort mendeteksi adanya serangan port scanning dengan uji coba variasi serangan sebanyak enam variasi yaitu scanning TCP scan yang ditentukan sebagai serangan medium, scanning UDP scan sebagai serangan medium, scanning Null Scan sebagai serangan high, scanning XMAS Scan sebagai serangan high, scanning FIN Scan sebahai serangan high dan terakhir scanning version dan OS medium.

Percobaan pertama dengan perintah scanning sebagai scanning Null scan, dengan menggunakan nmap dengan perintah scanning menggunakan –sN seperti pada gambar 16 berikut. Saat berhasil melakukan scanning maka akan tampil seluruh port yang terbuka pada LoRa Network Server dan Mac address dari device LoRa Netwrok server.

Pada percobaan pertama diatas akan dilakukan deteksi oleh snort sebagai serangan sehingga pada file output alert.csv akan terdapat notifikasi dari serangan tersebut seperti pada gambar 17 berikut. Terdeteksi adanya scanning Null scan dengan mematikan seluruh Flag dari port, selain itu dengan perintah –sN juga melalukan scanning dari port TCP sehingga oleh snort terdeteksi sebagai serangan rules Scanning port.



Gambar 16. Perintah Nmap Null Scan

```
06/24-11:56:15.876691 ,300005,192.168.43.98,192.168.43.68,"Nmap NULL Scan",TCP
06/24-11:56:15.876691 ,300003,192.168.43.98,192.168.43.68,"NMAP TCP Scan",TCP
```

Gambar 17. Output File Alert.csv Null Scan

Percobaan berikutnya dengan variasi command dari -sX, -sF, -sU, -sT dan –A, maka akan menghasilkan notifikasi pada output alert.csv berbeda. Pada gambar 18 merupakan hasil output dari scanning XMAS. Gambar 19 hasil output alert.scv dari FIN scanning dan gambar 20 Hasil dari scanning versi dan OS.

```
06/24-12:05:45.811488 ,300006,192.168.43.98,192.168.43.68,"Nmap XMAS Tree Scan",TCP
06/24-12:05:45.811488 ,300003,192.168.43.98,192.168.43.68,"NMAP TCP Scan",TCP
```

Gambar 18. Output File Alert.csv XMAS Scan

```
06/24-12:12:46.934293 ,300007,192.168.43.98,192.168.43.68,"Nmap FIN Scan",TCP
06/24-12:12:46.934293 ,300003,192.168.43.98,192.168.43.68,"NMAP TCP Scan",TCP
```

Gambar 19. Output File Alert.csv FIN Scan

```
06/24-12:18:51.033236 ,300003,192.168.43.98,192.168.43.68,"NMAP TCP Scan",TCP
06/24-12:18:54.023262 ,300004,192.168.43.68,192.168.43.1,"Nmap UDP Scan",UDP
06/24-12:20:19.171579 ,100002,192.168.43.98,192.168.43.68,"Ada Serangan Ping Medium",ICMP
06/24-12:20:19.171673 ,100002,192.168.43.68,192.168.43.98,"Ada Serangan Ping Medium",ICMP
06/24-12:20:19.218874 ,100002,192.168.43.98,192.168.43.68,"Ada Serangan Ping Medium",ICMP
06/24-12:20:19.219053 ,100002,192.168.43.68,192.168.43.98,"Ada Serangan Ping Medium",ICMP
06/24-12:20:19.242374 ,500002,192.168.43.98,192.168.43.68,"Flood UDP attack detected Medium",UDP
06/24-12:20:19.242503 ,100002,192.168.43.68,192.168.43.98,"Ada Serangan Ping Medium",ICMP
06/24-12:20:19.312202 ,300004,192.168.43.68,202.162.32.12,"Nmap UDP Scan",UDP
06/24-12:20:19.441146 ,500002,202.162.32.12,192.168.43.68,"Flood UDP attack detected Medium",UDP
06/24-12:20:20.761607 ,300004,192.168.43.68,192.168.43.1,"Nmap UDP Scan",UDP
06/24-12:20:20.765391 ,500002,192.168.43.1,192.168.43.68,"Flood UDP attack detected Medium",UDP
```

Gambar 20. Output File Alert.csv Versi dan OS Scan

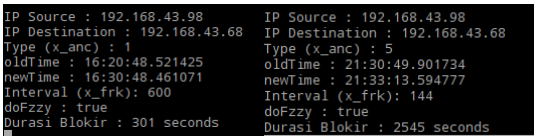
Percobaan keterbuktian snort selain berfungsi untuk menguji apakah snort berhasil melakukan scanning lalu lintas jaringan pada LoRa Network Server, juga melakukan analisa terkait dengan pengaruh terhadap bandwidth pada LoRaWAN seperti pada tabel 4.4 yang merupakan hasil dari simulasi pengujian sebanyak 6 kali percobaan dengan serangan variatif yaitu low, medium dan high secara random atau bebas dan dengan jenis serangan ping flooding. Hal ini dilakukan untuk membuktikan bahwa dengan adanya serangan serangan yang masuk pada LoRaWAN network server mampu mengganggu dari performansi LoRaWAN. Pada tabel 5 dibawah bandwidth, delay,jitter dan throughput diukur dengan adanya serangan ping flooding dengan data 65000 bytes.

Tabel 5. Pengujian Performa Setelah Serangan Ping Flooding

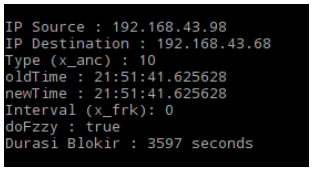
ke -	Bandwidth TX (kbps)	Bandwidth RX (kbps)	Delay (seconds)	Jitter	Throughput Bit/sec
1	388,01	385,48	0,011758	-0,0002245	1066000
2	476,09	463,49	0,034189	0,001338154	1079000
3	311,49	302,98	0,027773	0,005724333	1030000
4	474,14	461,67	0,02934	0,000148417	1041000
5	388,04	383,90	0,011603	-0,000311081	1013000
6	484,84	472,10	0,01042	0,000287	1059000
Rata2	420,44	411,60	0,020847	0,001117	1048000

4.6 Hasil Keterbuktian Metode Fuzzy

Pengujian fuzzy pada penelitian ini dengan menjalankan hostInspector.sh pada LoRa Server. Fuzzy dikatakan dapat berjalan apabila mampu melakukan perhitungn durasi block adanya serangan dan tetap dapat meneruskan aktifitas jaringan yang bukan merupakan serangan. Pada gambar 21 merupakan hasil dari hostInspector saat terdapat serangan dari mesin penyerang.



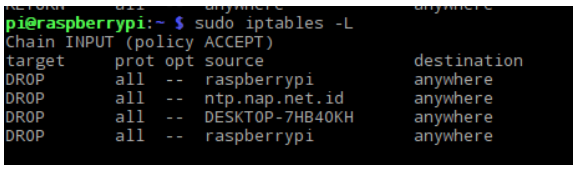
(a) (b)



(c)

Gambar 21. Output Defuzzy Durasi Blokir Low (a), Medium (b), High (c)

Hasil dari defuzzyfikasi akan dikirimkan perintah pada iptables, sehingga ditampilkan pada rule iptables akan terdapat beberapa perintah blok mesin penyerang seperti pada gambar 22 berikut dan apabila waktu sudah selesai dari durasi blokirnya maka rule dengan ip address tersebut akan di unblock.



Gambar 22. IPTables Block Attacker

Pada tabel 6 merupakan hasil pengujian dari metode fuzzy yang disesuaikan dengan rule seperti pada tabel 3.8 terkait rule evaluation. Dengan melakukan pengujian kedalam tiga jenis serangan yaitu Low, Medium dan High. Dan dengan frekuensi waktu berbeda dengan menguji dalam empat kelompok yaitu Jarang, Sedang, Sering dan Sangat Sering. Percobaan dilakukan sebanyak dua kali untuk memastikan data sebelum diambil suatu kesimpulan.

Tabel 6. Pengujian Metode Fuzzy

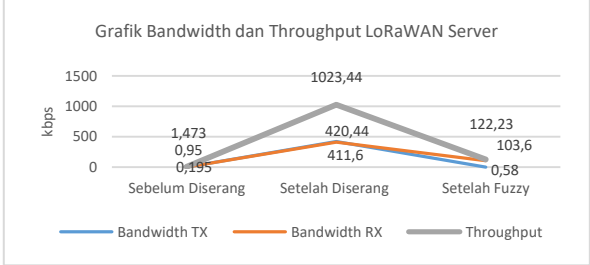
Rule Evaluation	Tipe Serangan	Durasi Block (seconds)
Serangan Low Frekuensi, Sangat Sering	Ping Flooding	3597
Serangan Medium, Frekuensi Sangat Sering	Ping Flooding	3597
Serangan High, Frekuensi Sangat Sering	Ping Flooding	3597
Serangan Low, Frekuensi : 600 s	UDP Flooding	301
Serangan Low, Frekuensi : 540 s	UDP Flooding	301
Serangan Low, Frekuensi : 360 s	UDP Flooding	903
Serangan Low, Frekuensi : 10 s	UDP Flooding	3567
Serangan Low, Frekuensi : 6 s	UDP Flooding	3597
Serangan Low, Frekuensi : 1 s	UDP Flooding	3597
Serangan Medium, Frekuensi : 600 s	UDP Flooding	301
Serangan Medium, Frekuensi : 540 s	UDP Flooding	301
Serangan Medium, Frekuensi : 360 s	UDP Flooding	903
Serangan Medium, Frekuensi : 10 s	UDP Flooding	3567
Serangan Medium, Frekuensi : 6 s	UDP Flooding	3597
Serangan Medium, Frekuensi : 1 s	UDP Flooding	3597
Serangan High, Frekuensi : 600 s	UDP Flooding	301
Serangan High, Frekuensi : 540 s	UDP Flooding	301
Serangan High, Frekuensi : 360 s	UDP Flooding	903
Serangan High, Frekuensi : 10 s	UDP Flooding	3567
Serangan High, Frekuensi : 6 s	UDP Flooding	3597
Serangan High, Frekuensi : 1 s	UDP Flooding	3597
TCP Scan	Scanning Port	2675
UDP Scan	Scanning Port	2675
XMAS Scan	Scanning Port	3597
FIN Scan	Scanning Port	3597
Null Scan	Scanning Port	2683
Versi dan OS Scan	Scanning Port	2766

Dalam penelitian ini membuktikan keberhasilan dan manfaat dari adanya metode fuzzy dalam snort, yaitu kenaikan bandwidth akibat adanya serangan yang dapat diatasi dengan adanya metode fuzzy. Pada tabel 7 dibawah ini menunjukkan bandwidth, delay, jiter dan throughput adanya fuzzy.

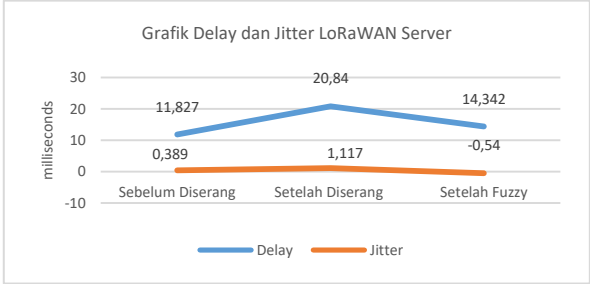
Tabel 7. Pengujian Performa Setelah Metode Fuzzy

ke-	Bandwidth TX (kbps)	Bandwidth RX (kbps)	Delay (seconds)	Jitter (seconds)	Througput Bit/sec
1	0,16	103,08	0,015759	-0,00063	110000
2	0,16	102,66	0,01275	-0,0005	119000
3	0,08	107,39	0,015529	-0,00049	112000
4	1,61	101,59	0,01352	-0,00053	110000
5	0,19	97,77	0,015661	-0,00059	190000
6	1,27	109,13	0,01283	-0,00052	110000
Rata – rata	**0,58**	**103,6**	**0,014342**	**-0,00054**	**125166,7**

Dari hasil tabel 7 terkait pengaruh performa dengan adanya serangan yang pada penelitian ini melakukan analisa bandwidth, delay, jitter dan throughput dari adanya serangan dari ping flooding maka dapat dilihat pada gambar 23 dan gambar 24 dibawah ini. Dari grafik dibawah ini terjadi penurun bandwidth, delay, jitter dan throughput akibat adanya blok dari source IP dengan kondisi mesin penyerang tetap melakukan serangan.



Gambar 23. Grafik Pengaruh Fuzzy Pada Banwidth dan Throughput

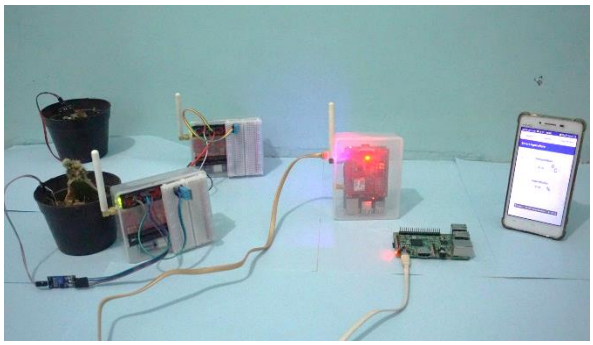


Gambar 24. Grafik Pengaruh Fuzzy Pada Delay dan Jitter

4.7 Hasil Portotype Alat

Portotype alat smart agriculture dalam penelitian terdiri dari LoRa Node yang merupakan kotak arduino, kotak lora dragino shield, sensor YL69, dan sensor DHT11. LoRa Node ini menggunakan daya sebesar 9 volt. Pada LoRa Gateway terdiri dari raspberry pi 3 model b, terdapat lora gps hat gateway. LoRa Gateway ini menggunakan daya sebesar 2,5 volt. Pada penelitian ini LoRaWAN Network Server diimplementasikan pada LoRa Gateway. Pada LoRa application server terdiri dari kota raspberry pi 3 model b dengan daya sebesar 2,5 volt, berisikan program script shell dan python untuk subscriber dan

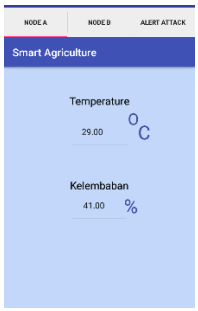
berisi database server. Tampilan alat secara kesuluruhan dapat dilihat pada gambar 25, dan dibuat seperti pada penerapan pada suatu tanaman dengan pembacaan sensor dari smartphone.



Gambar 25. Tampilan Alat Keseluruhan

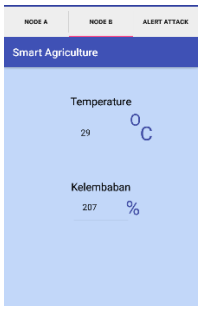
4.8 Hasil Tampilan Android

Hasil akhir dari penelitian ini, bahwa petani dan admin dapat memantau suhu dan kelembaban perkebunan strawberry dan notifikasi serangan terhadap LoRaWan server dapat selalui di pantau dalam aplikasi android. Sehingga data perkebunan dapat secara realtime dan juga pencegahan adanya serangan LoRa network server lebih terpantau. Tampilan aplikasi android yang dapat diakses oleh petani dan admin, tidak membutuhkan login untuk melihatnya. Cukup menginstall aplikasi smart agriculture pada smartphone. Gambar 26 merupakan tampilan dari LoRa node pertama atau lora node A, sehingga suhu dan kelembaban dapat dipantau seperti pada gambar berikut.



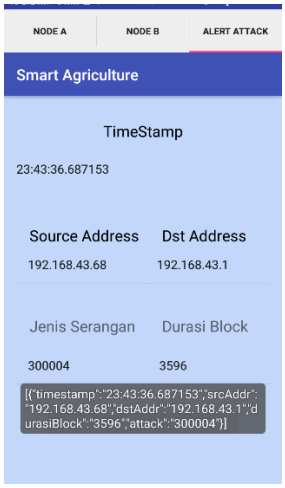
Gambar 26. Tampilan Android LoRa Node A

Tampilan pada node B sama seperti pada node A, tujuan dibedakan dalam dua tab agar lebih mudah dalam melakukan monitoring tiap LoRa nodenya, yang apabila kondisi dari antar node berjauhan. Gambar 27 merupakan tampilan dari LoRa node kedua atau lora node B, sehingga suhu dan kelembaban dapat dipantau seperti pada gambar berikut.



Gambar 27. Tampilan Android LoRa Node B

Pada tab terakhir dari aplikasi android penelitian ini menampilkan notifikasi serangan yang berisi waktu, jenis serangan, alamat IP sumber dan tujuan, dan juga hasil dari perhitungan algoritma fuzzy terkait durasi block juga dapat ditampilkan pada aplikasi android. Gambar 28 merupakan tampilan dari Alert Attack server.



Gambar 28. Tampilan Android Notifikasi Serangan

5. Kesimpulan

Dari keseluruhan hasil penelitian, dapat ditarik beberapa kesimpulan dan saran sebagai berikut.

5.1 Simpulan

Berdasarkan Hasil Penelitian Network Intrusion Detection System Berbasis Snort Dengan Metode Fuzzy Untuk Mengatasi Serangan Menggunakan Lorawan Pada Smart Agriculture dapat diambil kesimpulan sebagai berikut.

1. LoRaWAN Network Server saat kondisi normal dengan aktivitas jaringan untuk pengiriman data dari LoRa Shield menggunakan bandwidth transceiver sebesar 0,95 kbps dan bandwidth receiver 0,195 kbps.Dengan throughput sebesar 1437 bps
2. Pada saat terdapat serangan pada LoRaWAN Network server rerata bandwidth yang digunakan yaitu bandwidth transceiver sebesar 420,44 kbps dan bandwidth receiver 411,60 kbps. Dengan throughput sebesar 1048 kbps. Dan terdapat

peningkatan pada delay dan jitter yang memiliki nilai masing masing 0,02084 seconds dan 0,00117 seconds.

3. NIDS pada Snort dengan metode fuzzy dapat melakukan pemblokiran alamat ip penyerang dengan perhitungan durasi sesuai dengan rules yang ditentukan. Dengan durasi block antara 10 detik hingga 3600 detik sesuai perhitungan dari output defuzzyfikasi.
4. Aktivitas mencurigakan dalam lalu lintas jaringan pada LoRaWAN Network Server dengan nilai ancaman 1 sampai 10, dengan nilai 1 sebagai low attack dan 10 sebagai high attack. Dengan frekuensi waktu sebagai variabel himpunan fuzzy yaitu jarang / delay antara 360 s sampai 600 s, sedang / delay antara 6 s sampai 540 s, sering / delay antara 0 sampai 360 s dan sangat sering / delay antara 0 sampai 6 s.
5. Menggunakan Snort dengan metode fuzzy dapat mengoptimalkan performa dari LoRaWAN server yaitu dengan besar bandwidth transceiver 0,58 kbps dan bandwidth receiver sebesar 103,6 kbps. Throughput menurun kembali dengan nilai 122,233 kbps, dengan delay sebesar 14,342 milisecond dan jitter sebesar -0,54 milisecond.

5.2 Saran

Saran yang dapat digunakan untuk mengembangkan penelitian mengenai Network Intrusion Detection System Berbasis Snort Dengan Metode Fuzzy Untuk Mengatasi Serangan Menggunakan Lorawan Pada Smart Agriculture ialah.

1. Pengembangan sistem smart agriculture untuk penyiraman dan pencahayaan menggunakan LoRaWAN.
2. Menggunakan hardware dengan support dual channel sehingga dapat dilakukan penelitian pengaruh serangan, deteksi snort dan metode fuzzy pada saat komunikasi dua arah
3. Mengembangkan rules snort untuk deteksi serangan dari LoRaWAN Server.

Daftar Rujukan

[1] Al-Ali, A., Zualkeman, I. A., Gupta, R., & Karar, M. A. (2017). A Smart Home Energy Management System Using IoT and Big Data Analytics Approach. *IEEE Transactions on Consumer Electronics, 63, No.4*, 426-434.

[2] Alnabulsi, H., Islam, M. R., & Mamu, Q. (2014). Detecting SQL Injection attacks using SNORT IDS. *IEEE*.

[3] Alsubhi, K., Boutaba, R., & Al-Shaer, E. (2008). Alert prioritization in Intrusion Detection Systems. *IEEE*.

[4] Andrei, M. L., Radoi, A., & Tudose, S. (2017). Measurement of Node Mobility for the LoRa Protocol . *IEEE*.

[5] Budiman, S. A., Iswahyudi , C., & Sholeh, M. (2014). Implementasi Intrusion Detection System (IDS) Menggunakan Jejaring Sosial Sebagai Media Notifikasi. *Prosiding Seminar Nasional Aplikasi Sains and Teknologi* .

[6] Cox, E. (1994). The Fuzzy System Handbook. *Academic Press - Inc*.

[7] Dewi, E. K., & Kasih, P. (2017). Analisis Log Snort Menggunakan Network Forensik. *Jurnal Ilmiah Penelitian dan Pembelajaran Informatika, vol 2, no 2*.

[8] El-Hajj, W., Aloul, F., & Trabelsi, Z. (2008). On Detecting Port Scanning using Fuzzy Based Intrusion Detection System. *IEEE*.

[9] Elvira, F., Duskarnaen, M. F., Z, B., & Isharyanto, B. (2010). Sistem Keamanan Jaringan Komputer Dengan Menggunakan Firewall Iptables dan Snort. *Universitas Negeri Jakarta*.

[10] Kontogiannis, S., Kokkonis, G., Ellinidou, S., & Valsamidis, S. (2017). Proposed Fuzzy-NN Algorithm with LoRa Communication Protocol for Clustered Irrigation Systems. *MDPI, Future Internet*.

[11] Kuswardani. (2011). Sistem Deteksi Dan Penanganan Intruisi Menggunakan Snort dan Base Implementasi Pada Pt. Oasys Solusi Teknologi.

[12] Lavric, A., & Popa, V. (2017). LoRa Wide-Area Networks from an Internet of Things Prespective. *ECAI*.

[13] Nugroho, I. W., Harianto, & Mardiana, I. G. (2014). Rancang Bangun Aplikasi Intrussion Detection System Dengan Menggunakan Metode Fuzzy. *stikom, vol 3, no 1*.

[14] Sembiring, I., Widiasari, I. R., & Prasetyo , S. D. (2009). Analisa dan Implementasi Sistem Keamanan Jaringan Komputer dengan Iptables sebagai Firewall Menggunakan Metode Port Knocking. *Univeritas Kristen Satya Wacana*.

[15] Tiyas , F. I., Hadi, M. Z., & K, E. M. (2011). Aplikasi Web untuk Metode Fuzzy Neural Network pada Intrusion Detection System Berbasis Snort. *Pens Institut Teknologi Sepuluh Nopember Surabaya*.