Studi Analisis Algoritma Naïve Bayes Untuk Sistem Deteksi Intrusi Pada Internet Of Things

1st Muhammad Kana Riskilah
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
kanariskilah@students.telkomuniversity.ac.id

2nd Fazmah Arif Yulianto
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
fazmaharif@telkomuniversity.ac.id

line 1: 3rd Erwid M Jadied
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
jadied@telkomuniversity.ac.id

Abstrak

Internet of Things (IoT) merupakan sebuah alat yang mampu berkomunikasi dan mengirimkan data melalui jaringan tanpa interaksi dari manusia. Seiring berkembangnya jaman, penggunaan teknologi semakin banyak dimanfaatkan dan hal ini berpengaruh terhadap kebutuhan terhadap perangkat IoT yang membuat perangkat ini semakin berkembang luas penggunaannya. Dalam perkembangannya, masalah pada bidang privasi dan keamanan menjadi salah satu hal yang berbahaya dan harus menjadi fokus utama. Contoh serangan yang bisa menyerang perangkat IoT yakni dictionary attack, DDoS, mitm, dsb. Langkah yang bisa dilakukan untuk menghindari serangan tersebut adalah dengan menggunakan Intrusion Detection System (IDS). Tujuan dari penelitian ini adalah mencari model yang optimal untuk mendeteksi serangan dictionary attack dan DDoS dengan menggunakan metode algoritma machine learning (ML) naïve bayes pada Internet of Things (IoT) yang disimulasikan menggunakan node-red. Algoritma naïve bayes dipilih karena Intrusion detection system (IDS) membutuhkan tingkat performansi dan akurasi yang tinggi. Hasil dari penelitian ini berupa model yang optimal dan dibangun dengan algoritma naïve bayes yang diterapkan untuk Intrusion detection system (IDS) pada Internet of Things (IoT) dengan hasil akurasi untuk dataset yang diambil pada penelitian ini 99.30% untuk DDoS dan 99.74% untuk dictionary attack sedangkan untuk dataset yang diambil dari penelitian[19][20] 82.38% untuk DDoS dan 79.88% untuk dictionary attack. Kata kunci : IoT, IDS, dictionary attack, DDoS, naïve bayes.

Abstract

Internet of Things (IoT) is a tool that is able to communicate and transmit data over a network without human interaction. Along the times, the use of technology is increasingly being used and this affects need for IoT devices which makes these devices increasingly widely used. In its development, issues in the field of privacy and security have become one of the most dangerous and must be main focus. Examples of attacks that can attack IoT devices are Dictionary attacks, DDoS, mitm,etc. Steps that can be taken to avoid these attacks are to use Intrusion Detection System (IDS). The purpose of this study is to find optimal model for detecting dictionary and DDoS attacks using the naïve bayes machine learning method on the IoT which is simulated using node-red. The Naïve Bayes algorithm was chosen because the IDS requires high level of performance and accuracy. The results of this study are in form of optimal model and built with the naïve bayes algorithm which is applied to IDS on IoT with accuracy results for the dataset taken in this study 99.30% for DdoS, 99.74% for Dictionary attack while for dataset taken from research[19[20] 82.38% for DdoS, 79.88% for Dictionary attack.

Keywords: IoT, IDS, dictionary attack, DDoS, naïve bayes.

I. PENDAHULUAN

A. Latar Belakang

Teknologi *Internet of Things* (IoT) pertama kali diperkenalkan oleh Kevin Ashton pada tahun 1999. Konsep IoT ini diartikan sebagai sebuah kemampuan untuk menghubungkan objek yang cerdas dan memungkinkannya untuk berinteraksi dengan objek lain, lingkungan, maupun dengan peralatan komputasi cerdas lainnya melalui jaringan internet[1]. Perangkat IoT merupakan perangkat yang *flexible* dan dapat digunakan untuk membantu aktivitas manusia. Dan pada saat ini, perangkat *Internet of Things* (IoT) memiliki kemampuan transfer data untuk berkomunikasi antar perangkat.

Didalam proses komunikasi dan transfer data ini rentan sekali terjadinya serangan terhadap perangkat maupun jaringan. Maka dari itu, keamanan merupakan aspek penting yang harus dijaga didalam sebuah sistem. Sebuah sistem, selain harus memberikan pengalaman yang baik untuk pengguna, juga harus memberikan jaminan rasa aman kepada pengguna dari ancaman penyerang yang tidak bertanggung jawab. Oleh karena itu, dibutuhkan adanya sistem yang bisa

mendeteksi serangan sejak dini untuk memperkecil kemungkinan serangan. *Intrusion detection system* (IDS) merupakan sebuah sistem yang berfungsi untuk mengidentifikasi *traffic* atau lalu- lintas pada jaringan yang disini merupakan jaringan *Internet of Things* (IoT) dimana *intrusion detection system*

(IDS) dapat menentukan apakah *traffic* atau lalu-lintas aman, mencurigakan, atau terindikasi merupakan sebuah serangan [2]. Maka dari itu, dibutuhkan klasifikasi serangan yang nanti akan dipakai pada *Intrusion detection system* (IDS) dengan memetakan anomali yang mencurigakan dan sedang terjadi didalam lalu-lintas data.

Penelitian ini berfokus pada bagaimana mencari model yang optimal untuk serangan *dictionary attack* dan *distributes denial of service* (DdoS) proses publish-subscribe untuk menjalankan fungsi internet of things (IoT). Sebelum lanjut ke proses publish-subscribe ada proses otentikasi terlebih dahulu. Pada tahap otentikasi ini dictionary attack bisa menyerang dengan cara mengacak password yang ada di wordlist dan diulang sampai ketemu. Pada protokol MQTT juga rentan terjadi DDoS. Serangan ini mengganggu alur kerja dari sebuah jaringan dengan mengeksploitasi perangkat dan sistem untuk mengakses sumber daya. Dengan

B. Topik dan Batasannya

Berdasarkan masalah yang diangkat pada latar belakang diatas, penelitian ini memiliki perumusan masalah tentang bagaimana melakukan studi analisis dan analisis performansi terhadap algoritma naïve bayes dengan membandungkan isi serta hasil terhadap dataset yang berbeda untuk menghasilkan tingkat akurasi serangan terhadap IDS. Berdasarkan latar belakang dan rumusan tersebut, penelitian ini memiliki batasan masalah sebagai berikut :

Menggunakan algoritma ML (machine learning) naïve bayes

Jenis serangan meliputi dictionary attack dan DDoS

Pengujian hanya dilakukan pada lingkup protokol MQTT

C. Tujuan

Tujuan dari penelitian ini adalah untuk melakukan studi analisis dengan menggunakan algoritma naïve bayes pada dataset yang berbeda. Sehingga didapatkan akurasi untuk masing-masing dataset, maka diharap penelitian mendapatkan model yang optimal untuk diterapkan pada IDS (intrusion detection system) device IoT.

D. Organisasi Tulisan

Jurnal penelitian ini akan berisi 5 bab, yaitu Bab 1-akan membahas mengenai latar belakang, rumusan masalah, dan tujuan pengerjaan tugas akhir ini. Bab 2-membahas fakta dan teori yang berkaitan dengan perancangan sistem untuk mendirikan landasan berfikir. Dengan menggunakan fakta dan teori yang dikemukakan pada bab ini penulis menganalisis kebutuhan akan rancangan arsitektur sistem yang dibangun. Bab 3-menjelaskan metode penelitian, rancangan sistem dan metode pengujian yang dilakukan dalam penelitian. Bab 4-berisi tentang

.

yang terjadi pada *internet of things* (IoT) dengan menggunakan algoritma naïve bayes. Pada perangkat *Internet of Things* (IoT),komunikasi berjalan melalui sebuah *gateway*. *Gateway* yang disebutkan disini biasa dikenal dengan sebutan *broker*. Di dalam *broker* ini berjalan layanan yang menggunakan protokol MQTT sebagai pusat komunikasi. Pada protokol MQTT ini terjadi

menggunakan bot akan cenderung mudah dilakukan dan dengan dampak yang menyeluruh dalam artian menghancurkan infrastruktur agar alur kerja program tidak dapat berjalan.

Dari sekian banyak classifier yang ada, naïve bayes adalah metode yang dipilih untuk penelitian ini karena naïve bayes memberikan algoritma yang sederhana dan memberikan asumsi kuat bahwa atribut independent memiliki kelas juga proses perhitungan cepat[3].

evaluasi dan analisis dari hasil penelitian yang telah dilakukan. Bab 5-berisi tentang kesimpulan dari penelitian.

II. KAJIAN TEORI

A. Penelitian terkait

Pada penelitian yang dilakukan[1], berkembangnya teknologi membuat munculnya ancaman terhadap device internet of things (IoT). Ada beberapa saja tipikal serangan yang sudah ditangani dan beberapa sisanya masih belum. Butuh perhatian khusus dari komunitas seperti akademisi, peneliti, bahkan industri.

Pada penelitian yang dilakukan[2], menggunakan naïve bayes untuk mengklasifikasikan serangan-serangan baru pada intrusion detection system (IDS) dan menghasilkan akurasi antara 81-84.67%.

Pada penelitian[3], dijelaskan bahwa naïve bayes merupakan algoritma pembelajaran sederhana yang menjadikan semua class memiliki keterkaitan dengan atribut independen.

Pada penelitian[4], semakin banyaknya perangkat pintar yang mampu berkomunikasi didalam jaringan banyak serangan-serangan yang berhasil dicatat. Metode uintuk melindungi dari serangan ini menggunakan value to keyed hash dengan pemetaan kode value to HMAC. Metode ini ideal untuk industri, dimana node perlu terbagi menjadi sensor dan pengontrol. Serta kunci dan permintaan publikasi yang perlu dikelola untuk melindungi dari serangan DDoS.

Pada penelitian[5], dictionary attack merupakan serangan sederhana dan mudah dilakukan selama sistem keamanan dari suatu sistem terhadap suatu ppassword tidak diproteksi dengan standar yang baik maka dari ancaman yang sederhana akan menjadi ancaman yang serius

Pada penelitian[6], menggunakan mekanisme *blockchain* untuk melindungi perangkat *internet of things* (IoT) karena catatan tiap transaksi yang dilakukan disimpan di *blockchain* dan terhubung ke server. Hal tersebut membuat akan lebih ter organisir.

Pada penelitian[7], *internet of things* (IoT) menawarkan kemajuan revolusioner dalam banyak konteks, tetapisesuatu yang terhubung ke internet akan mendapatkan kerentanan akan serangan. Kerentanan terhadap SQL *injection* membuat botnet rentan terhadap serangan balik. *Malware mirai* yang diujikan memindai alamat IP dengan *username* dan *password default* pabrik sehingga menjadikan lebih mudah diperbaiki.

Pada penelitian[8], mengusulkan sistem MQTT menggunakan otentikasi OTP sebagai pengaman dan mencegah dari serangan *brute force.* Percobaan menggunakan google *authentication* dapat efektif mencegah dan mengamankan serangan dictionary attack pada MQTT.

Pada penelitian yang dilakukan[9], beberapa percobaan telah dilakukan dan dievaluasi ditimbang dari berbagai pengklasifikasi pembelajaran mesin berdasarkan intrusi KDD Himpunan data. Hal ini berhasil menghitung beberapa kinerja metrik untuk mengevaluasi pengklasifikasi yang dipilih. Untuk algoritma naive bayes mendapatkan akurasi sebesar 98.9%.

Pada penelitian yang dilakukan[10], mengusulkan membuat IDS untuk *internet of things* (IoT) dengan berfokus menggunakan alogitma machine learning Naive Bayes dan menghasilkan akurasi sebesar 94.80%.

Pada penelitian yang dilakukan[11], mengklasifikasikan anomali IDS menggunakan algoritma klasifikasi Na¨ıve Bayes dari hasil pemilihan atribut dengan teknik korelasi correlationbased feature selection. Nilai akurasi yang diperoleh sebesar 74.8%.

Pada penelitian yang dilakukan[12], mengusulkan taksonomi IDS yang dibutuhkan objek data sebagai dimensi utama untuk mengklasifikasikan dan merangkum metode pembelajaran mesin dan mendalam sebagai 5 literatur IDS. Akurasi yang dihasilkan yakni 99.62% dan false alarm rate of 1.57% pada the KDD99 dataset.

Pada penelitian yang dilakukan[13], dilakukan tes dengan menggunakan dataset tentang sekumpulan serangan terhadap MQTT dan menggunakan beberapa metode *machine learning*, didapatkan akurasi sebesar 98.9% untuk MQTT dataset dengan algoritma naïve bayes. Sebagai pembandingnya, didapatkan akurasi 64.3% untuk naïve bayes dengan dataset yang sudah *balanced*.

Pada penelitian yang dilakukan[14], disebutkan bahwa banyak terdapat kelemahan pada protocol MQTT yang bisa dieksploitasi oleh serangan DDoS. Serangan yang dilakukan menggunakan *SlowITe* yang menargetkanprotokol MQTT dan menggunakan pendekatan tingkat rendah.

Pada penelitian yang dilakukan[15], DDoS ini berkembang seiring dengan perkembangan sistem operasi Windows. Banyak alat dan teknik untuk menyerang, menembus, dan membuat lumpuh suatu sistem. Yang sering terkena dampaknya adalah suatu sistem dengan skala yang besar. Serangan DDoS biasanya bertujuan untuk mematikan sebuah layanan yang dikerjakan dari komputer atau jaringan yang diserang. Dampaknya akan terasa sangat besar bagi sebuah perusahaan atau instansi.

Pada penelitian[16], *brute force* terjadi karena tidak adanya enkripsi ketika menjalankan proses *three way handshake*. Kemanan dilakukan dengan SNORT, dan hasilnya SNORT dapat mendeteksi serangan serta dapat menghasilkan peringatan pada deteksi.

B. *Internet of Things* (IoT)

Menurut Kevin Ashton(2009) Secara umum internet of things merupakan sebuah konsep yang bertujuan untuk memperluas manfaat dari konektivitas internet yang tersambung secara terus-menerus memungkinkan daya pengendalian, komunikasi, kerja sama dengan berbagai perangkat keras, berbagi data, memvirtualisasikan segala hal nyata ke dalam bentuk internet, melalui jaringan internet atau disebut juga M2M.

C. Dictionary attack

Dictionary attack adalah sebuah pendekatan yang *straightforward* untuk memecahkan suatu masalah, biasanya didasarkan pada *problem statement* dan definisi konsep yang dilibatkan. Secara garis besar, penyerang akan mencoba mendapatkan akses yang sah dengan cara menebak *username* dan *password*. *Dictionary attack* tidak berbeda jauh dari *brute force* karena pada dasarnya teknik ini merupakan pengembangan dari *brute force*. *Dictionary attack* tidak mencoba kombinasi satu per satu karakter yang ada melainkan mencoba kombinasi kata berdasarkan *list of word* atau *wordlist*[5].

D. *Distributed denial of service* (DDoS)

DDoS merupakan serangan yang mempunyai ciri menyerang secara terang-terangan untuk menggagalkan tujuan layanan yang sah. Tujuan utama dari DDoS yakni untuk menghancurkan infrastruktur sistem dengan cara membanjiri aliran data pada sistem tersebut sehingga sistem menjadi berat untuk melakukan pekerjaannya. DDoS akan mencegah alur kerja dengan banyak entitas dari penyerang[6].

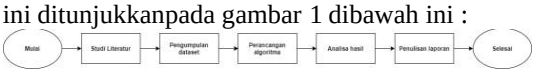
a. Naïve bayes

Naive bayes *classifier* termasuk teknik prediksi berdasarkan probabilitas sederhana pada teorema Bayes. Nilai probabilitas dalam metode ini digunakan sebagai pengambilan keputusan karena setiap kasus terdapat proses komputasi resiko [11].

III. METODE

A. *Framework* penelitian

Dalam pelaksanaan penelitian ini, metodologi yang dilakukan dalam menyelesaikan penilitian ini ditunjukkanpada gambar 1 dibawah ini :



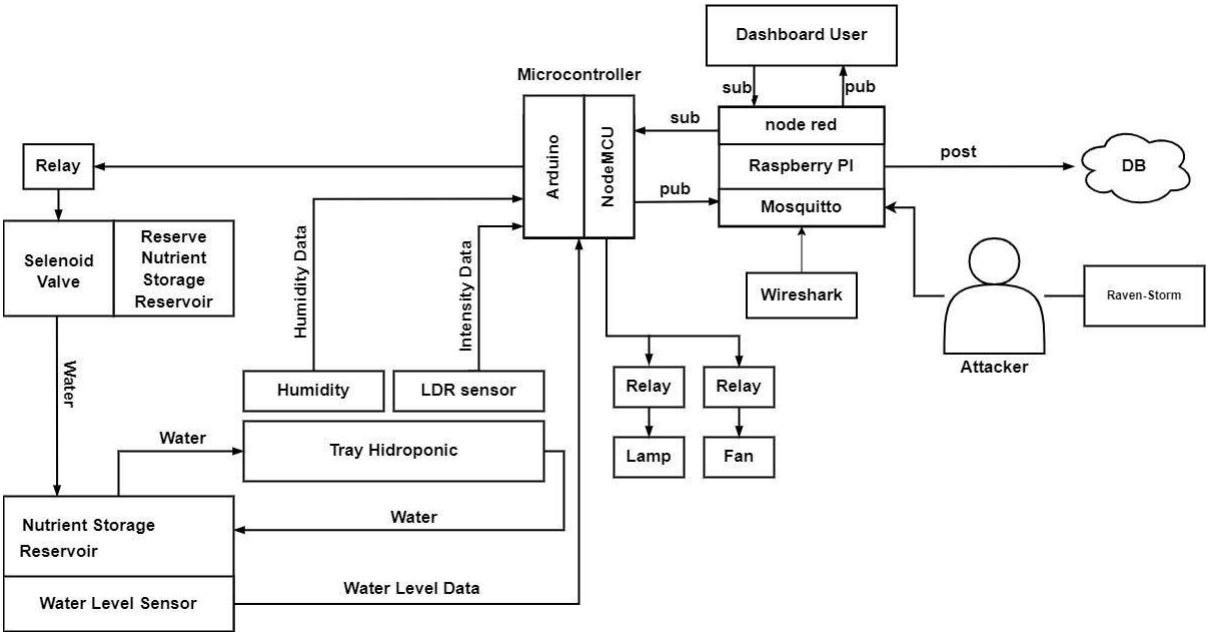
Gambar 1. Diagram alur penelitian

Berikut penjelasan dari masing-masing tahapan riset pada gambar 1:

1. Studi Literatur, pada tahap ini dilakukan review terhadap penilitian-penelitian terkait yang telah dilakukan sebelumnya, merangkum fakta serta teori yang dibutuhkan untuk penelitian. Langkah pertama yang dilakukan adalah memilih jurnal dengan usia maksimal 10tahun ke belakang kemudian dipelajari dan dianalisa sehingga didapatkan benang merah tentang permasalahan yang harus diselesaikan.

3.1 Gambaran sistem

2. Pengumpulan dataset adalah proses dalam mengambil dataset dari yang sudah ada lewat internet dan pengumpulan dataset sendiri dari MQTT yang nanti akan digunakan sebagai data untuk penelitian.
3. Perancangan algoritma, pada tahap ini penulis melakukan klasifikasi terhadap dataset dengan algoritma naïve bayes untuk mendapatkan akurasi yang paling tinggi yang dapat diusulkan.
4. Pengujian dan Analisis hasil, pada tahap ini penulis melakukan pengujian terhadap performansi algoritma terhadap dataset. Hasil dari tahap ini adalah nilai-nilai performansi dari algoritma yang digunakan.
5. Penulisan Laporan Pada tahap ini penulis menyusun laporan terkait penelitian yang dilakukan mengikuti metodeperancangan tata tulis ilmiah. Hasil dari tahapan ini adalah buku TA.

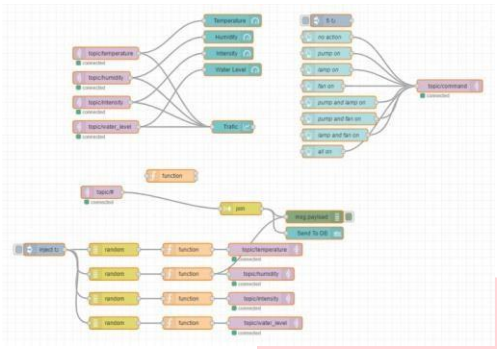


Gambar 2. Topologi *internet of things* (IoT)

Gambar 2 diatas menunjukkan topologi *Internet of Things* (IoT) yang digunakan dan berfungsi untuk menjalankan sebuah sistem hidroponik. Letak MQTT terdapat pada broker mosquito didalam Raspberry. Protokol tersebut berjalan didalam broker mosquito yang dimana broker menjadi penyedia layanan dari MQTT. Tugas dari MQTT yakni berperan sebagai penghubung transaksi data *publish* dan *subscribe*. *Attacker* menggunakan komputer dan *tools* Raven-Storm[18] untuk menyerang. Fokus *attacker* menyerang pada MQTT, karena didalamnya terdapat proses komunikasi data. Kemudian untuk mendapatkan data *traffic* ketika

MQTT sedang diserang, menggunakan wireshark yang sudah di *install* pada raspi sebagai *single-board circuit*
karena wireshark mampu untuk melakukan *capture* terhadap *traffic* yang berjalan.

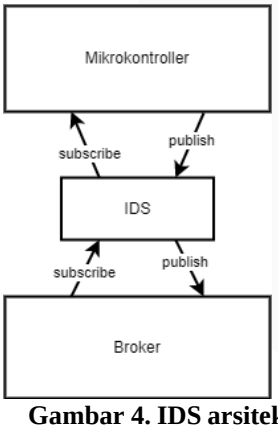
3.1.1 Node-Red



Gambar 3. Simulasi menggunakan node-red

Dalam tugas akhir ini, simulasi dari *Internet of Things* (IoT) dilakukan menggunakan node-red. Node- red berfungsi untuk melakukan simulasi transaksi *publish* dan *subscribe* dan menunjukkan *flow* data sesuai dengan topologi pada gambar 2. Jadi, untuk pengambilan data pada penelitian ini menggunakan data yang disimulasikan pada node-red. Seperti yang terlihat pada gambar 3 diatas.

B. *Intrusion detection system* (IDS) arsitektur



Gambar 4. IDS arsitektur

Berdasarkan topologi yang sudah digambarkan sub-bab 3.2, mqtt berada pada broker yang berjalan menggunakan raspberry. Disini adalah jembatan komunikasi antara sensor, database, dan dashboard untuk menentukan action apa yang akan dilakukan selanjutnya. Menerapkan IDS (*Intrusion Detection System*) dengan cara melakukan model yang sudah di training dengan dataset sebelumnya kedalam broker server. Jadi, sebelum ada transaksi masuk ke broker, di cek terlebih dahulu menggunakan IDS (*Intrusion detection system*). Jadi, setiap *traffic* atau transaksi data yang masuk pada mqtt akan terlebih dahulu melewati IDS. Model akan mendapat fitur-fitur yang diperlukan dari setiap transaksi publish subscribe secara *real-time* dan fitur tersebut juga sama dengan yang didapat dari proses *training.* Fitur-fitur yang didapat secara *real-time* ini yang akan diklasifikasikan dan output berupa *alert* mencurigakan dari *traffic* yang sedang berjalan. Seperti yang terlihat pada gambar 4 diatas.

C. Data

Data yang digunakan terbagi menjadi 2, yakni data yang diambil sendiri dan data yang sudah ada sebelumnya[19][20] yang nanti akan digunakan sebagai pembanding. Untuk data penelitian sebelumnya, mengambil data [19] untuk *dictionary attack* dan [20] untuk DDoS. Untuk *dictionary attack* terdapat 5.000 baris data, sedangkan untuk DDoS terdapat 94.626 baris data. Pada dataset yang diambil pada penelitian ini, untuk

dictionary attack terdapat 150.064 baris data dan DDoS terdapat 15.046 baris data. Data yang diambil penelitian ini diambil untuk digunakan sebagai pembanding terhadap dataset[19][20] dan dapat diambil benang merah atas *feature* yang akan digunakan.

i. Data *collecting*

Untuk mendapat data, penulis melakukan serangan terhadap protokol MQTT dengan tipe serangan *dictionary attack* dan DDoS. Ketika diserang, *capture* data dilakukan dengan menggunakan *tools* wireshark.

1. Dictionary attack

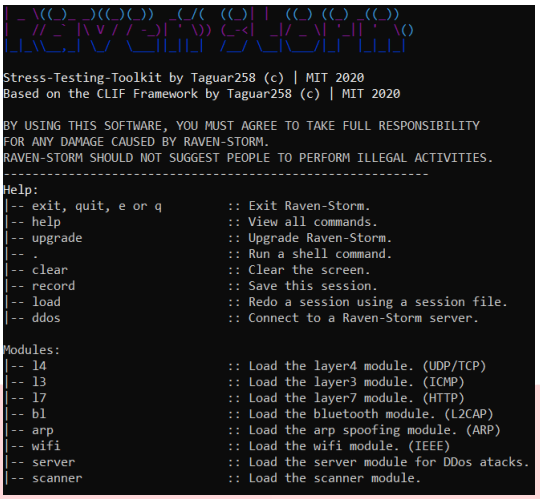
```
1  foreach username dalam wordlist-username do
2  |  foreach password dalam wordlist-password do
3  |  |  temp = isLogin(username, password)
4  |  |  if temp:
5  |  |  // berhasil
6  |  |  break
7  |  end
8  end
```

Gambar 5. Algoritma *dictionary attack*

Didalam serangan *dictionary attack*, menggunakan *wordlist* untuk menebak *username* dan *password* yang digunakan didalam protokol MQTT. Dikarenakan untuk setiap transaksi *publish-subscribe* diperlukan *username* dan *password* untuk otentikasi, maka poin itulah yang menjadi target dari *dictionary attack*. Seperti yang digambarkan pada gambar 5. Didalam gambar 5 dijelaskan bahwa untuk mendapatkan *username* dan *password* algoritma dilakukan pencocokan hasil dengan yang ada didalam variabel isLogin. Jika terdapat kecocokan antara kalimat yang ada di *wordlist* yang telah dimasukkan dengan

variabel tersebut maka perulangan akan berhenti sesuai.
dan menampilkan *username* dan *password* yang

2. Distributed denial of service (DDoS)



Gambar 6. Tampilan serangan DDoS menggunakan Raven-Storm

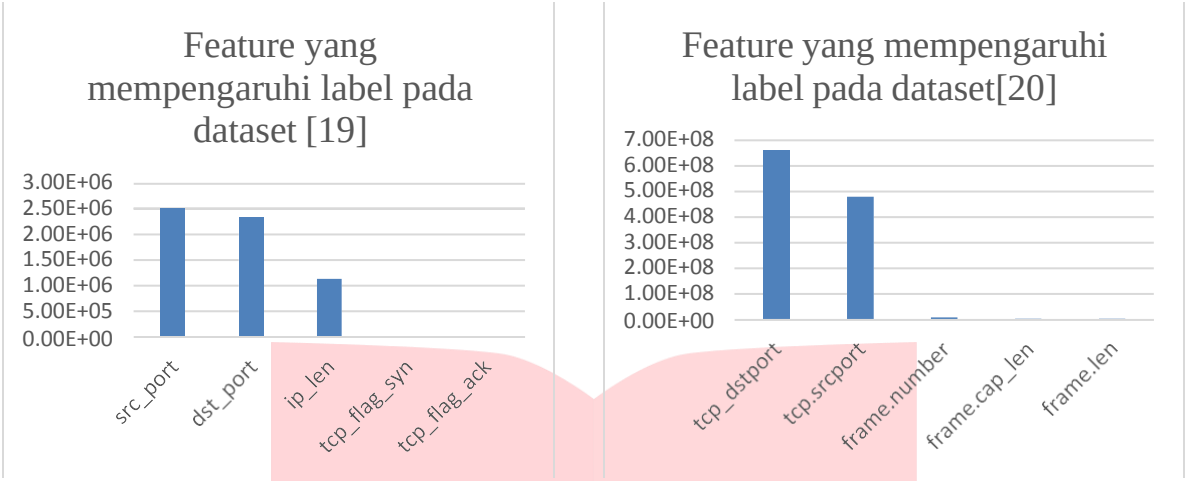
Didalam serangan *Distributed denial of service* (DDoS), dilakukan menggunakan tools yang bernama Raven- Storm[18].

ii. Feature selection

Dilakukan *feature selection* untuk mengetahui *feature* yang berpengaruh terhadap label. Pada penelitian ini menggunakan teknik *univariate feature selection*, yakni dengan memilih fitur berdasarkan statistik univariate dan hanya dikeluarkan feature yang memiliki score tertinggi. Score didapatkan atas dasar keterkaitan atribut dengan kelas nya serta keterkaitan antar atribut[21].

D. Dataset [19][20]

Teknik *univariate feature selection* digunakan pada dataset[19][20]. Teknik ini digunakan karena menentukan *ranking* secara independen antara *feature* satu dan yang lain sehingga memudahkan untuk memilih dan mengesampingkan *feature* dengan *ranking* yang rendah.



Gambar 7. *Feature* yang paling berpengaruh terhadap label pada dataset [19][20]

Pada gambar 7 dijelaskan 5 *feature* yang berpengaruh pada dataset[19]20] setelah dilakukan teknik *univariate feature selection.* Garis horizontal dibawah menunjukkan nama *feature*, sedangkan garis vertikal di samping menjelaskan tentang *score* pada masing-masing *feature*.

Tabel 1. Deskripsi *feature* gambar 7

Feature	Data Type	Description
src_port	Integer	Port asal
dst_port	Integer	Port yang dituju
ip_len	Integer	Panjang paket
tcp_flag_syn	Binary	Sinkronisasi TCP flag
tcp_flag_ack	Binary	Indikasi transmisi pada TCP
tcp_dstport	Integer	Port tujuan TCP
tcp_srcport	Integer	Port asal TCP
frame.number	Integer	Nomor frame
frame.cap_len	Integer	Panjang frame jaringan cap
frame.len	Integer	Panjang frame

Pada tabel 1 dijelaskan tentang deskripsi dari masing-masing *feature* pada dataset[19][20] sesuai dengan gambar 7.

E. Dataset yang diambil pada penelitian ini

Dataset yang diambil pada penelitian ini tidak menggunakan *feature selection* dikarenakan hanya ada 3 *feature* dan semua *feature* yang ada didalam dataset yakni Source, Destination, dan Protokol berpengaruh terhadap label. Label merupakan penanda apakah serangan atau bukan. Ditandai dengan tipe data binary 0 untuk non-serangan dan 1 untuk serangan.

Tabel 2. Deskripsi *feature* dataset yang diambil pada penelitian ini

Feature	Data Type	Description
Source	Text	IP asal
Destination	Text	IP yang dituju
Protokol	Integer	Protokol yang digunakan

Pada tabel 2 dijelaskan tentang deskripsi dari masing-masing *feature* pada dataset yang diambil pada penelitian ini.

F. Metrik Uji

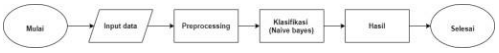
Metrik pengujian yang digunakan dalam melakukan pengujian algoritma adalah metrik yang digunakan pada penelitian-penelitian sebelumnya, seperti pada gambar 8.

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN}$$

Gambar 8. Rumus metrik uji

TP melambangkan total dari kebenaran yang diklasifikasikan serangan (*True-Positive*) dan TN (*True-Negative*) melambangkan total dari kejadiaan normal yang diklasifikasikan sebanyak Nsampel. Sedangkan FP (*False-positive*) melambangkan total kebenaran yang salah diklasifikasikan dan FN (*False-negative*) melambangkan total dari kejadian normal yang salah diklasifikasikan (*False-positive* dan *False-Negative*).

G. Skenario pengujian



Gambar 9. Gambaran umum skenario pengujian

Gambar 9 diatas menjelaskan tentang bagaimana proses untuk mencapai tujuan pada penelitian ini. Langkah pertama, adalah melakukan *input* dari dataset. Kemudian dilakukan *preprocessing* dimana pada tahap ini dilakukan pembersihan data agar siap untuk diklasifikasi. Didalamnya terdapat proses seleksi fitur, yakni menghitung skor untuk masing-masing fitur dan diambil 5 fitur dengan skor terbesar untuk selanjutnya dipakai pada proses klasifikasi. Selanjutnya adalah proses klasifikasi yang menggunakan algoritma naïve bayes. Tahap yang terakhir, yakn mendapatkan hasil yang nanti akan menunjukkan akurasinya. Didalamnya menggunakan metode *cross validation* agar akurasi lebih akurat.

IV. HASIL DAN PEMBAHASAN

A. Hasil Pengujian

Pada pengujian ini, dilakukan perbandingan antara dataset yang diambil dari penelitian [19][20] serta dataset yang diambil pada penelitian. Perbandingan ini ditampilkan berdasarkan akurasi. Hasil yang ditampilkan dalam bab ini merupakan hasil yang didapatkan setelah melalui skenario pengujian seperti yang dijelaskan pada bab 3.5. Hasil ditampilkan dalam tabel 1 dibawah ini :

Tabel 3. Hasil perbandingan

	Dataset [19][20]	**Dataset sendiri**
Dictionary attack	79.88%	99.74%
Distributed denial of service	82.38%	99.30%

Seperti yang dijelaskan pada tabel 1, masing-masing dari hasil menampilkan hasil yang berbeda. Untuk dataset yang diambil dari internet, menghasilkan 79.88% untuk *dictionary attack* dan 82.83% untuk DDoS. Sedangkan dalam dataset yang diambil sendiri, menghasilkan 99.74% untuk *dictionary attack* dan 99.30% untuk DDoS.

B. Analisis Hasil Pengujian

i. Tahapan klasifikasi

Pada tahapan klasifikasi, terdapat beberapa proses. Proses yang terdapat pada tahap ini *preprocessing* dan klasifikasi. Pada tahap *preprocessing* adalah tahap untuk pembersihan data agar data siap diklasifikasi. Pada tahap ini menggunakan teknik *oversampling*, *feature selection* serta pemberian label secara manual untuk serangan dan bukan serangan. Pada tahap klasifikasi dilakukan klasifikasi dan menghasilkan akurasi, dilakukan pula teknik *cross validation* agar mendapatkan akurasi terhadap label yang lebih akurat.

C. Pemberian label

Pemberian label manual hanya dilakukan terhadap dataset yang diambil dalam penelitian ini karena untuk dataset[19][20] sudah terdapat label secara *default*. Pemberian label dilakukan berdasarkan *feature* ip_src,ip_dst,protokol karena ip_src,ip_dst,protokol yang terdapat sudah *default* dan jika terdapat isi dari *feature* selain itu bisa diindikasikan merupakan anomali serangan. Isi *default* dari *feature* bisa dilihat seperti pada gambar 9.

Tabel 4. Isi *feature* default untuk dataset yang diambil pada penelitian ini

ip_src	127.0.0.1
ip_dst	127.0.0.1
Protokol	MQTT,TCP

Tabel 5. Contoh anomali serangan

ip_src	ip_dst	protokol
192.168.0.106	239.255.255.250	SSDP
172.18.16.1	239.255.255.250	SSDP
192.168.20.1	239.255.255.250	SSDP
192.168.56.1	239.255.255.250	SSDP

Tabel 3 dinyatakan sebagai anomali dikarenakan isi *feature* tidak sesuai dengan *default* yang tersebut pada tabel 2. Data tersebut berdasarkan data yang diambil pada penelitian ini.

D. Oversampling

Dalam melakukan pengujian, dilakukan teknik oversampling dikarenakan data mengalami *imbalanced*. Berikut jumlah baris data sebelum dilakukan *oversampling*.

Tabel 6. Jumlah baris data sebelum oversampling

	Dataset[19][20]	Dataset sendiri
Dictionary attack	142 : 4.857 (baris data)	136.090 : 13.973 (baris data)
Distributed denial of service	49.111 : 45.514 (baris data)	480 : 14.565 (baris data)

Tabel 7. Jumlah baris data setelah oversampling

	Dataset[19][20]	Dataset sendiri
Dictionary attack	4.857 : 4.857 (baris data)	136.090 : 136.090 (baris data)
Distributed denial of service	49.111 : 45.514 (baris data)	14.565 : 14.565 (baris data)

Berdasarkan data diatas, terlihat bahwa data normal banding(:)serangan perbandingan cukup jauh. Untuk meminimalisir agar tidak berpangaruh terhadap akurasi, maka dilakukan teknik *oversampling*. Jadi dengan teknik ini, rasio yang kecil disamakan sejumlah rasio yang besar secara random dengan smote.

E. Feature Selection

Feature Selection merupakan sebuah teknik yang penting dalam *pre-processing*. Teknik ini berfungsi untuk mengurangi jumlah fitur yang berpengaruh terhadap label dengan mengurangi fitur yang tidak relevan serta data yang berlebih. Tujuannya adalah untuk memilih *feature* terbaik dari suatu kumpulan *feature* dengan memberikan *score* terhadap masing-masing *feature*.

F. Klasifikasi

Pada proses klasifikasi menggunakan model GaussianNB, dimana model ini menghitung keterkaitan antara variabel independen terhadap kelas. Algoritma ini cenderung cepat karena mudah untuk menunjukkan bahwa paling tidak sering ada korelasi antar variabel di kehidupan nyata.

$$P(C_k \mid x) = \frac{P(C_k) * P(x \mid C_k)}{P(x)}$$

Gambar 10. Rumus pengklasifikasian naïve bayes[10]

Pada gambar 10 dijelaskan rumus tentang klasifikasi menggunakan naïve bayes. Penjelasan masing-masing atribut sebagai berikut :

a. **P(C|x)** adalah probabilitas posterior kelas C (target yang layak) berdasarkan prediktor x (atribut /variabel independen);
b. **P(C)** adalah probabilitas prior kelas C;

c. **P(x|C)** adalah kemungkinan, yang merupakan probabilitas dari prediktor x pada kelas C;
d. **P(x)** adalah probabilitas prior dari prediktor x;
e. **k** hanyalah notasi untuk membedakan antara kelas yang berbeda karena setidaknya ada 2kelas terpisah dalam skenario klasifikasi.

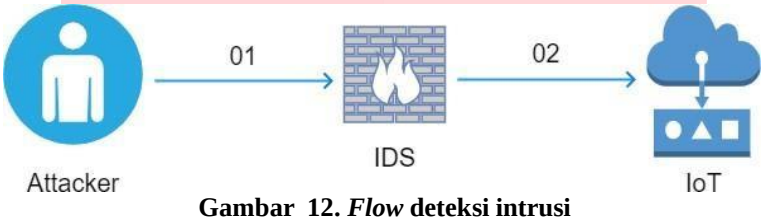
2. Cross validation

Cross validation merupakan metode statistik untuk mengevaluasi kinerja model algoritma dimana data akan dipisah menjadi 2 subset yakni data latih dan data uji. Disini penulis membagi data menjadi 5, 1 akan menjadi data uji dan 4 sisanya akan menjadi data latih. Tujuan dari *cross validation* ini untuk menemukan kombinasi terbaik untuk akurasi. Rumus bisa dilihat pada gambar 11 dibawah ini :

$$CV = \frac{1}{k}\sum_{i=1}^{k} CV_i$$

Gambar 11. Rumus *cross validation*

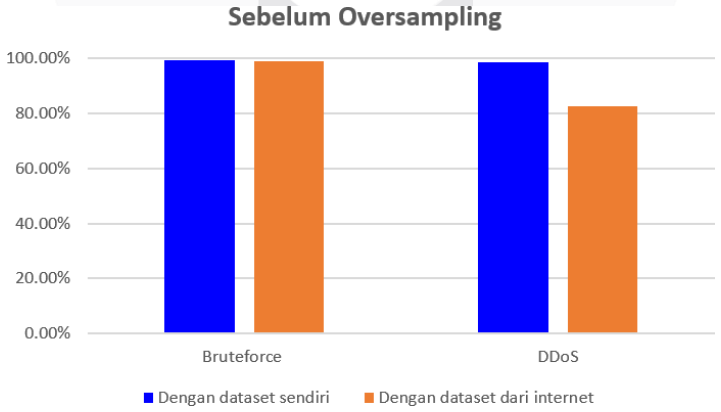
ii. Tahapan deteksi



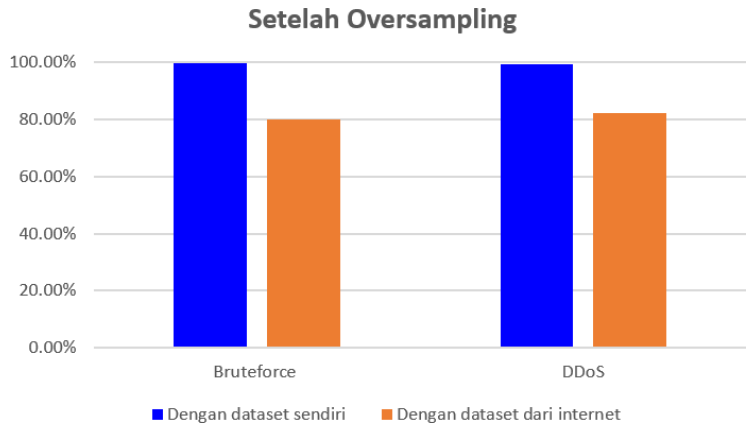
Gambar 12. *Flow* deteksi intrusi

Pada gambar 12 menjelaskan tentang tahapan deteksi intrusi pada *Internet of Things* (IoT). Pada poin 01 *attacker* akan melakukan sebuah *request* dengan membawa data seperti yang terdapat pada sub bab 3.4.2. Kemudian, pada *intrusion detection system* (IDS) akan melakukan pengecekan anomali *request* data yang dikirimkan oleh *attacker*. Selanjutnya, *intrusion detection system* (IDS) akan melakukan pengecekan dengan model *machine learning* yang telah ditanamkan. *Intrusion detection system* (IDS) akan melakukan pengecekan terhadap *feature* sesuai dengan yang ada pada data *train* seperti ip dan protokol yang sudah pasti ada pada setiap transaksi. Jika *request* yang dikirimkan oleh *attacker* dianggap anomali oleh *intrusion detection system* (IDS), maka *request* tersebut akan ditolak dan tidak dilanjutkan ke *device Internet of Things* (IoT).

b. Grafik hasil pengujian



Gambar 13. Diagram hasil pengujian sebelum dilakukan *oversampling* dan dengan *cross validation*



Gambar 14. Diagram hasil pengujian sebelum dilakukan *oversampling* dan dengan *cross validation*

Dari perbandingan gambar 13 dan 14 diatas, terlihat perubahan yang cukup signifikan antara dataset sendiri dengan dataset[19][20]. Pada dataset yang diambil sendiri, untuk *dictionary attack* dari 99.52% menjadi 99.74% setelah dilakukan *oversampling* dan untuk DDoS dari 98.64% menjadi 99.30% setelah dilakukan *oversampling*. Sedangkan pada dataset yang diambil dari internet, untuk *dictionary attack* dari 98.96% menjadi 79.88% setelah dilakukan *oversampling* dan untuk DDoS dari 82.76% menjadi 82.38% setelah dilakukan *oversampling*. Semua hasil diatas sudah dilakukan pula teknik *cross validation*.

V. KESIMPULAN

Berdasarkan penelitian yang dilakukan oleh penulis, dari hasil pengujian dan analisis dapat disimpulkan bahwa algoritma *machine learning* naïve bayes dapat diaplikasikan untuk sistem deteksi intrusi (IDS) khususnya serangan *dictionary attack* dan *distributed denial of service* (DDoS) pada protokol MQTT. Hasil dari pengujian yang dilakukan, penelitian dengan menggunakan dataset yang diambil pada penelitian ini memiliki akurasi yang lebih tinggi dibandingkan dengan dataset yang diambil dari penelitian [19][20]. Hasil dari pengujian, yakni 99.30% untuk DDoS dan untuk *dictionary attack* 99.74% sedangkan untuk dataset yang diambil dari penelitian [19][20] untuk DDoS 82.38% dan untuk *dictionary attack* 79.88%.

Akan tetapi, terdapat perbedaan dalam jumlah *feature* yang terdapat dalam kedua dataset. Dalam dataset yang diambil sendiri, hanya terdapat 6 *feature* yang nantinya akan menjadi variabel *independent*. Akan tetapi, didalam dataset yang diambil dari [19][2], jumlah *feature* lebih banyak dibanding dengan data yang diambil terhadap penelitian ini. Hal ini memungkinkan untuk menjadi faktor yang akan mempengaruhi akurasi didalam klasifikasi.

Adapun saran dari penulis berdasarkan kekurangan diatas, yakni :

1. Penelitian yang lebih kompleks dengan menggunakan protokol MQTT dengan menggunakan perangkat yang lebih nyata agar didapat hasil yang lebih maksimal
2. Kedepannya, akan ada lebih banyak jenis-jenis algoritma *machine learning* yang lain yang bisa jadi jauh lebihoptimal dibanding menggunakan algoritma naïve bayes

REFERENSI

[1] Najib Warsun, and Selo Sulistyo. "Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things." *Jurnal Nasional Teknik Elektro dan Teknologi Informasi* 9.4 (2020): 375-384.

[2] Prasetyo, Arief, Luqman Affandi, and Dedi Arpandi. "Implementasi metode naive bayes untuk intrusion detection system (ids)." *Jurnal Informatika Polinema* 4.4 (2018): 280-280.

[3] Webb, Geoffrey I., Eamonn Keogh, and Risto Miikkulainen. "Naïve Bayes." *Encyclopedia of machine learning* 15 (2010): 713-714.

[4] Hindy, Hanan, et al. "Machine learning based IoT Intrusion Detection System: an MQTT case study (MQTT- IoT-IDS2020 Dataset)." *International Networking Conference*. Springer, Cham, 2020.

[5] Achmady, Sayed. "Analysis Dictionary Attack Dan Modifikasi Password Cracking Serta Strategi Antisipasi." *Jurnal Sains Riset* 7.1 (2017).

[6] Munshi Asmaa, Nouf Ayadh Alqarni, and Nadia Abdullah Almalki. "Ddos attack on IoT devices." *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 2020.

[7] Hallman, Roger, et al. "IoDDoS-the internet of distributed denial of sevice attacks." *2nd*

international conference on internet of things, big data and security. SCITEPRESS. 2017.

[8] Fauzi, Azwar Fatwa, Parman Sukarno, and Aulia Arif Wardana. "Otentikasi Pada Internet-of-things Berbasis Mqtt Menggunakan One-time-password Pada Kasus Iot Home Gateway." *eProceedings of Engineering* 6.2 (2019).

[9] Almseidin, Mohammad, et al. "Evaluation of machine learning algorithms for intrusion detection system." *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*. IEEE, 2017.

[10] Nandhini, P., M. Senthil, and S. Darsniya. "A network intrusion detection system for IoT using machine learning and deep learning approaches." *Int. J. Adv. Sci. Technol.* 29.3 (2020): 1017-1023.

[11] Anwar, Saipul, Fajar Septian, and Ristasari Dwi Septiana. "Klasifikasi Anomali Intrusion Detection System (IDS) Menggunakan Algoritma Naïve Bayes Classifier dan Correlation-Based Feature Selection." *Jurnal Teknologi Sistem Informasi Dan Aplikasi* 2.4 (2019): 135-140.

[12] Liu, Hongyu, and Bo Lang. "Machine learning and deep learning methods for intrusion detection systems: A survey." *applied sciences* 9.20 (2019): 4396.

[13] Vaccari, Ivan, et al. "MQTTset, a new dataset for machine learning techniques on MQTT." *Sensors* 20.22(2020): 6578.

[14] Vaccari, Ivan, Maurizio Aiello, and Enrico Cambiaso. "SlowITe, a novel denial of service attack affecting MQTT." *Sensors* 20.10 (2020): 2932.

[15] Hermawan, Rudi. "Analisis Konsep dan Cara Kerja Serangan Komputer Distributed Denial of Service (DDOS)." *Faktor Exacta* 5.1 (2015): 1-14.

[16] Stiawan, Deris, et al. "Investigating dictionary attack attack patterns in IoT network." *Journal of Electrical and Computer Engineering* 2019 (2019).

[17] Nugroho, Edi Dwi, Aji Gautama Putrada, and Andrian Rakhmatsyah. "Predictive Control on Lettuce NFT- based Hydroponic IoT using Deep Neural Network." *2021 International Symposium on Electronics and Smart Devices (ISESD)*. IEEE, 2021.

[18] Taguar258. "Raven-Storm". https://github.com/Taguar258/Raven-Storm.

[19] Hanan Hindy, Christos Tachtatzis, Robert Atkinson, Ethan Bayne, Xavier Bellekens.