p-ISSN: 2301-5373
e-ISSN: 2654-5101

Implementasi Algoritma Naive Bayes Classifier (NBC) Dan Information Gain Untuk Mendeteksi DDoS

Ida Bagus Gagananta Amartya [a1], I Made Widiartha [a2], I Gusti Agung Gede Arya Kadyanan [a3], I Gusti Ngurah Anom Cahyadi Putra [a4], I Putu Gede Hendra Suputra [a5], Cokorda Rai Adi Pramartha [a6].
[a]Informatics Engineering, Faculty of Math and Science, University of Udayana
South Kuta, Badung, Bali, Indonesia
[1]ibgagananta11@gmail.com
[2]madewidiartha@unud.ac.id
[3]gungde@unud.ac.id
[4]anom.cp@unud.ac.id
[5]hendra.suputra@unud.ac.id
[6]cokorda@unud.ac.id

Abstract

In this study, feature selection was also carried out using the information gain method, the result of feature selection improve the performance of DDoS attack detection against the Naive Bayes Classifier classification algorithm. The results obtained in this study are system testing on the results of the comparison of data performance that has been selected using 17 features and without the application of information gain feature selection using 43 features of course different, there are superior results from the application of Information Gain feature selection with an average accuracy value of 75.81 %, while the results obtained without the application of feature selection are 75.57%. The average precision level system performance using 17 features is 91.61%, while average precision result using 43 features is 92.20%. For the average recall value using 17 features, it is 57.63%, and results recall uses 43 features by 57.31%. In terms of execution time, the time required to execute the program using 17 features is faster and more effective, namely 89.17 seconds, while the program execution time using 43 features is longer, namely 205.34 seconds.

Keywords : *Naive Bayes Classifier , Information Gain, DDoS, Classification, K-Fold Cross Validation.*

1. Pendahuluan

Pada era globalisasi ini keamanan jaringan merupakan aspek penting dalam bidang teknologi informasi. Dari waktu ke waktu semakin banyak celah keamanan jaringan yang ditemukan dan disalahgunakan oleh para penjahat elektronik. Serangan terhadap jaringan komputer khususnya internet mengalami peningkatan. Internet tidak lagi hanya digunakan sebagai sarana bertukar informasi, dan juga mulai digunakan untuk keperluan komersial, misalnya sebagai sarana transaksi pembayaran. Hal ini tentu menyebabkan sejumlah besar data berharga semakin banyak beredar melalui jaringan komputer , salah satunya internet. Serangan yang dikirimkan terkadang susah dideteksi sehingga membuat tingkat keamanan dari jaringan komputer sangatlah tidak aman. Untuk meminimalisir resiko dari serangan, maka sistem pendeteksi serangan diperlukan untuk mendeteksi lalu lintas jaringan yang ada, dan dari klasifikasi ini dimungkinkan untuk mengetahui apakah aktivitas pada jaringan tersebut merupakan serangan.

Serangan Distributed Denial of Service (DDoS) merupakan serangan yang dikirimkan dari beberapa penyerang terhadap sebuah komputer atau server dalam jumlah yang melebihi kemampuan komputer itu sendiri [1]. Berdasarkan penelitian yang telah dilakukan terkait mengklasifikasi *Anomaly Intrusion Detection System (IDS)* menggunakan algoritma pengklasifikasi *Naive Bayes* dan pemilihan fitur berbasis korelasi, penelitian ini menggunakan pengumpulan data sistem deteksi intrusi UNSW-NB15. Hasil evaluasi menggunakan algoritma *Naive Bayes* untuk klasifikasi anomali IDS mencapai akurasi 71,2% sebelum atribut diseleksi dengan teknik terkait. Sedangkan untuk hasil klasifikasi, jika ada atribut yang dipilih oleh teknologi terkait di depan, maka diperoleh tingkat akurasi sebesar 74,8%.[2]. Jadi penulis akan

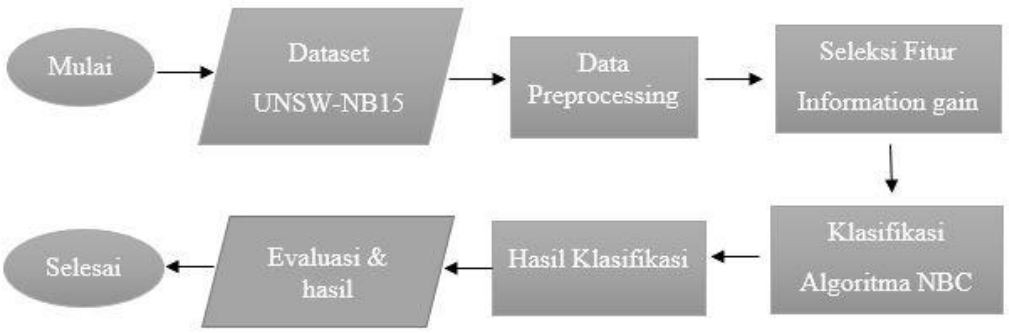
menggunakan metode *Naïve Bayes Classifier* menggunakan teknik seleksi fitur untuk mendeteksi serangan DDoS agar meningkatkan performa akurasi seperti penelitian sebelumnya. Disisi lain, ini menjadi tantangan untuk deteksi serangan karena lebih banyak informasi (fitur) akan diproses. Pada dasarnya tidak semua fitur yang terdapat pada trafik akan berdampak pada algoritma pendeteksian. Namun, pengetahuan diperlukan untuk menentukan tanda tangan yang benar dan relevan untuk mendeteksi serangan seperti DDoS. Karena sulit membedakan DDoS dari trafik normal. Terlalu banyak fitur yang tidak relevan menyebabkan kategori kelas yang tidak relevan. Dikemukakan bahwa pemilihan fitur dapat meningkatkan akurasi algoritma klasifikasi,[3] sehingga penelitian ini bertujuan untuk meningkatkan kinerja pendeteksian serangan DDoS menggunakan teknik pemilihan fitur perolehan informasi.

Dalam peneltian ini penulis memanfaatkan UNSW-NB15 sebagai dataset. Dataset ini dipilih karena dataset baru dikembangkan pada tahun 2015, yang terdiri dari kombinasi data serangan normal yang disintesis normal modern dan kontemporer, dimana pada penelitian sebelumnya dataset yang digunakan yaitu KDD Cup 1999 dan NSL-KDD yang merupakan dataset lama sehingga kurang akurat jika dilakukan pengujian deteksi serangan saat ini. Hasil nilai percobaan seleksi fitur dan tanpa seleksi fitur di bandingkan sehingga mendapatkan hasil akhir seberapa besar penerapan seleksi fitur terhadap *Naive Bayes Classifier* menggunakan data set UNSW-NB15 untuk mendeteksi serangan DDoS.

2. Metode Penelitian

Pada penelitian ini dataset yang akan digunakan adalah dataset UNSW-NB15 yang diambil pada situs website https://research.unsw.edu.au/projects/unsw-nb15-dataset. Dataset ini dipilih karena dataset baru dikembangkan pada tahun 2015, yang terdiri dari kombinasi data serangan normal yang disintesis normal *modern* dan kontemporer. Jenis data yang digunakan dalam penelitian ini yaitu data sekunder. Data sekunder adalah data yang sudah ada, yang dikumpulkan oleh lembaga dan organisasi penyelidik sebelumnya. Pengklasifikasian ini dimulai dengan memasukan dataset serangan DDoS, dataset tersebut kemudian diproses kedalam tahap *preprocessing.*

Pada dataset UNSW-NB 15 dibagi menjadi 70% data *train* dan 30% data *test* . Selanjutnya dilakukan seleksi fitur menggunakan teknik *Information Gain* untuk menghasilkan fitur yang relevan dan mengurangi fitur yang memiliki relevansi kecil agar meningkatkan nilai akurasi. Setelah di seleksi fitur dari dataset nya akan dilakukan proses klasifikasi dengan algoritma *Naïve Bayes Classifier* (NBC). Hasil klasifikasi digunakan sebagai prediksi kelas normal dan serangan. Tahap terakhir yaitu output evaluasi yang dilakukan pada metode *naive bayes classifier* dari suatu model klasifikasi dapat diukur dengan tingkat akurasi berdasarkan *confusion matrix*.



Gambar 1. *Flowchart* alur proses penelitian

Dataset ini memiliki 175341 *records* data. Dataset akan terbagi menjadi data *training* ,yang digunakan untuk menyeleksi fitur, membuat kelas dari dataset oleh metode *Information Gain*, *Naive Bayes Classifier*(NBC), dan data *testing* digunakan untuk mengevaluasi keakuratan model . Kemudian sistem membagi kumpulan data secara acak kedalam kereta dengan

p-ISSN: 2301-5373
e-ISSN: 2654-5101

menggunakan metode *K-Fold Cross Validation.* Dapat dilihat pada Tabel 1. yang merupakan jumlah *records* data serangan dan normal.

Tabel 1. Jumlah Paket Data

No	Nama	Jumlah *Records*
1	Normal	56000
2	Serangan	119341
Total *Records*		175341

2.1 Serangan Distributed Denial of Service (DDoS)

Serangan *Distributed Denial of Service* (DDoS) merupakan serangan yang mudah dilakukan namun sulit untuk ditanggulangi . Sebelum melakukan serangan DDoS, penyerang akan menyiapkan komputer untuk membantu dalam penyerangan tersebut. Komputer-komputer yang membantu dalam penyerangan tersebut disebut dengan komputer zombie atau botnet, dimana komputer tersebut dikendalikan oleh sebuah *server* atau komputer utama untuk membantu menyerang korban dan mengakibatkan *server* menjadi *down* dan mengakibatkan *system error* [4] .

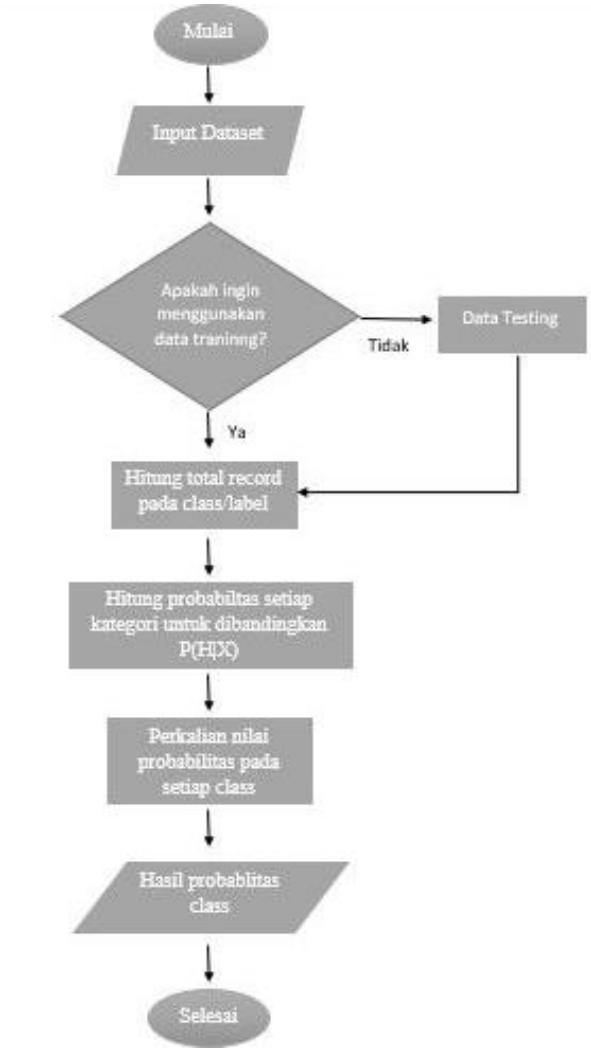
2.2 Naive Bayes Classifier

Naive Bayes Classifier selanjutnya disebut NBC termasuk teknik prediksi berdasarkan probabilitas sederhana pada teorema Bayes.Naive bayes adalah teknik penalaran probabilitas melalui kumpulan probabilitas yang dihitung dan menjumlahkan frekuensi dan kombinasi koleksi data. Nilai probabilitas dalam metode ini digunakan sebagai penentuan keputusan karena setiap kasus terdapat proses komputasi resiko. Persamaan *Naïve Bayes* diperoleh dari rumus bayes berikut (1) [5].

$$P(H|X)=P(X|H)P(H)P(X) \quad (1)$$

X = Dataset kelas tidak diketahui
H = Hipotesis kelas teridentifikasi
P (H | X) = Probabilitas H pada X (persentase H dalam X)
P (X | H) = Probabilitas konfirmasi X pada H (persentase bilangan X pada H)
P (H) = Probabilitas sebelum H
P (X) = Probabilitas sebelum X

Adapun flowchart dari *naive bayes* yang digunakan oleh peneliti, dapat dilihat pada Gambar 2. Berikut penjelasan flowchart *naive bayes* yaitu,tahapan pertama masukkan dataset berupa *csv *training* dan *testing* yang akan diproses di sistem. Setelah input data training dan *testing*, selanjutnya menghitung total *record* pada *class/label* dataset dan kelas tersebut dihitung probabilitasnya disetiap kategori untuk dibandingkan. Setelah menghitung probabilitas disetiap kategori, akan dilakukan perkalian nilai probabilitas pada setiap kelas dan menghitung jumlah kasus perkelas disetiap kategori. Tahap terakhir menghitung nilai presentase dan bandingkan hasil per kelas.



Gambar 2. *Flowchart* Klasifikasi *Naive Bayes Classifier*

2.3 Klasifikasi

Klasifikasi adalah metode yang dipakai untuk mencari sekelompok model (fungsi) sebagai deskripsi dan pembeda antar kelas-kelas data agar model tersebut dapat digunakan untuk memprediksi objek yang belum diketahui kelasnya atau memprediksi kecondongan data-data yang dihasilkan di waktu mendatang [6]. Klasifikasi mempunyai dua tugas utama, yaitu membangun *model* sebagai contoh, dan melakukan identifikasi/prediksi berdasarkan *model* yang sudah dibuat terhadap objek data baru yang dihasilkan di waktu mendatang, berada pada kelas mana kah objek data baru tersebut.

2.4 Seleksi Information Gain

Seleksi fitur digunakan untuk menghilangkan atau mengurangi fitur yang tidak relevan dalam proses klasifikasi. Proses perhitungan *Information Gain* akan dilaksanakan pada seluruh data dengan mengukur efektifitas suatu atribut atau fitur. Atribut dengan informasi tertinggi akan dipilih. Perhitungan IG didefinisikan dengan rumus (2) [3].

$$Entropy\ (S) = \sum_{i=1}^{n} - Pi*log2\ \text{p}i \qquad (2)$$

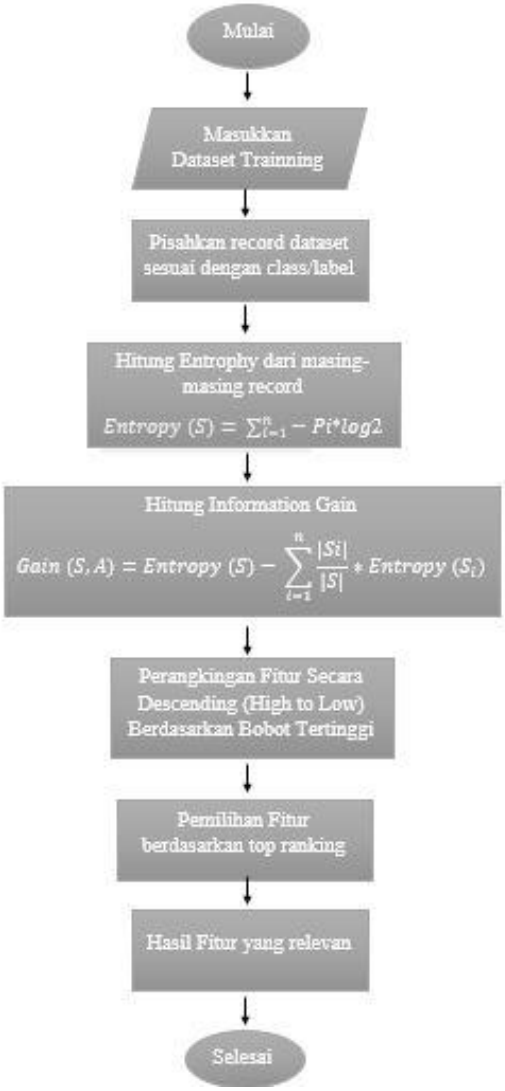
Keterangan :
n= Jumlah nilai yang ada pada atribut target (jumlah kelas klasifikasi)
pi = Jumlah sampel untuk kelas i

Kemudian nilai information gain yang digunakan untuk mengukur efektifitas suatu atribut dalam pengklafikasian data dapat dihitung dengan rumus di bawah ini (3).

p-ISSN: 2301-5373
e-ISSN: 2654-5101

$$Gain\ (S,A) = Entropy\,(S) - \sum_{i=1}^{n} \frac{|Si|}{|S|} * Entropy\ (S_i) \quad (3)$$

Keterangan :
S = Himpunan kasus
A = Atribut
n = jumlah partisi atribut A
$|Si|$ = jumlah kasus pada partisi ke-i
$|S|$ = jumlah kasus dalam S



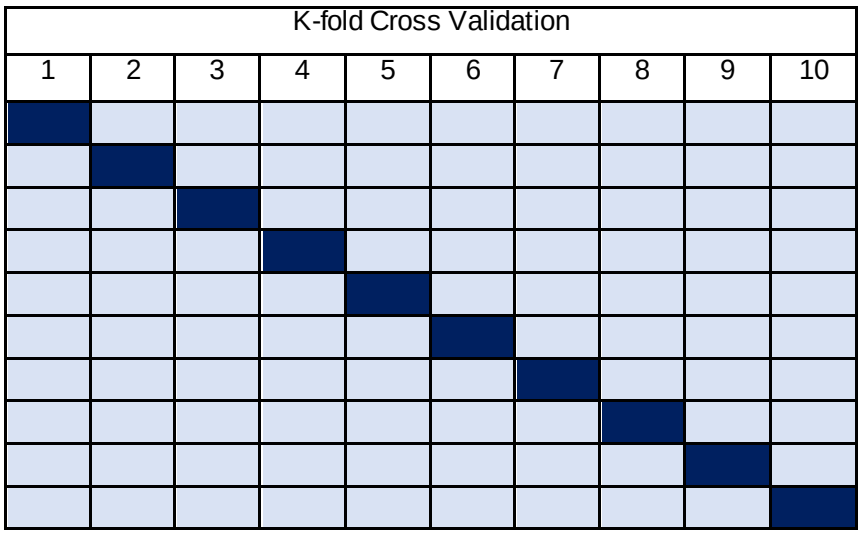
Gambar 3. *Flowchart* Proses Seleksi *Fitur Information Gain*

Teknik seleksi fitur ini dilakukan untuk mengurangi fitur yang tidak relevan dan mengurangi dimensi fitur pada data. Setelah melakukan perhitungan terhadap 49 fitur pada dataset UNSW-NB15, akan diterapkan teknik seleksi fitur *Information Gain* dengan metode perangkingan fitur terbaik setelah itu fitur yang diambil untuk melakukan klasifikasi sebanyak 49 fitur yang memiliki nilai *entrophy information gain* yang tertinggi atau skor yang terbaik.

2.5 K-fold cross validation

Cross validation adalah suatu teknik validasi model yang dilakukan untuk menilai hasil analisis secara akurat [7]. Metode ini memecah data menjadi k bagian set data dengan ukuran yang sama. Penggunaan *k-fold cross validation* untuk menghilangkan bias pada data. Pelatihan dan pengujian dilakukan sebanyak k kali. Pada percobaan pertama, subset S1 diperlakukan sebagai data pengujian dan subset lainnya diperlakukan sebagai data pelatihan, pada percobaan kedua subset S1, S3, sampai Sk menjadi data pelatihan dan S2 menjadi data pengujian, dan setererusnya [8]. Contoh *K-fold Cross Validation* dengan nilai k sama dengan 10.

Tabel 2. *K-fold cross validation*



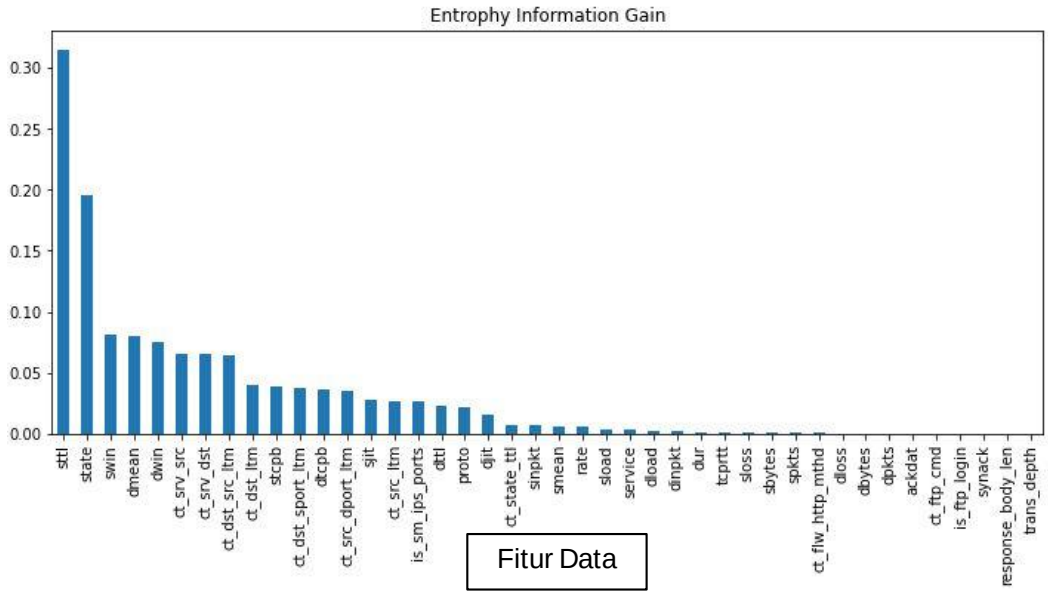
3. Hasil dan pembahasan

Dalam penelitian ini, penulis menggunakan data yang berasal dari UNSW-NB15 dengan jumlah 175341 *record* data. Dataset yang digunakan dalam penelitian terdiri dari 49 fitur yang mempunyai label/class 1 data normal dan 9 *type* serangan, yaitu *fuzzers*, *analysis*, *backdoors*, DoS, *exploits*, *generic*, *reconnaissance* , *shellcode*, dan jenis serangan *worms*. Pada tahapan ini dibutuhkan inputan data berupa file dataset yang memiliki format *.csv. Dalam penelitian ini mempunyai dua proses utama yang akan dijalankan. Proses pertama sistem melakukan seleksi fitur dari setiap atribut dataset yang digunakan agar menghasilkan fitur yang relevan dan mengurangi fitur yang memiliki relevansi kecil menggunakan metode *Information Gain*. Proses kedua sistem melakukan klasifikasi terhadap dataset, dimana data diklasifikasi kedalam 2 label yaitu normal dan serangan. Pada proses pembentukan klasifikasi diperlukan adanya proses diskritisasi.

Dalam proses perancangan sistem ini disebuah lingkungan komputer dengan spesifikasi perangkat keras Intel Core-i7 dengan RAM 4GB, HDD storage 1TB dan Graphic NVIDIA GEFORCE. Sistem ini diimplementasikan dengan bahasa pemograman python. Dalam perancangan dan implementasi sistem, digunakan beberapa perangkat lunak untuk memenuhi kebutuhan implementasi sistem. Berikut adalah spesifikasi perangkat lunak yang digunakan dalam penelitian :

1 Sistem Operasi Windows 10 64 bit
2 Google Chrome
3 Google Collaboratory
4 Notepad

p-ISSN: 2301-5373
e-ISSN: 2654-5101



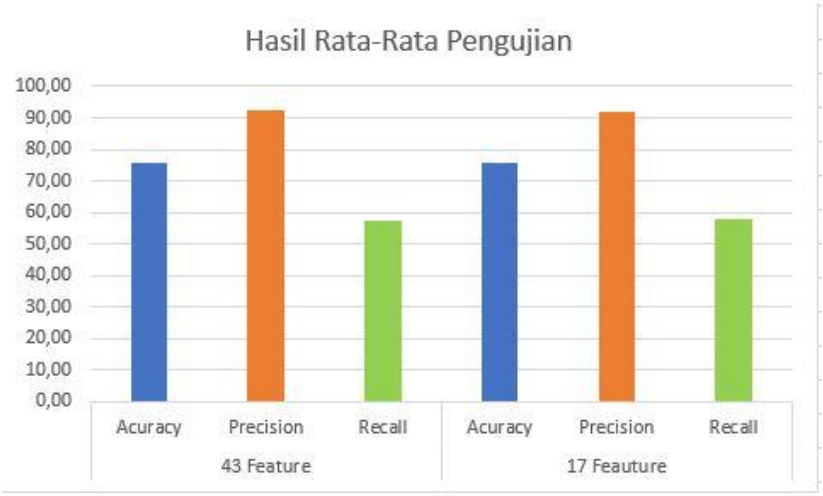
Gambar 4. Grafik Seleksi Fitur *Information* Gain

Dapat dilihat hasil nilai *entrophy* dari *information gain* berdasarkan perangkingan nilai fitur tertinggi hingga terendah. Dari hasil tersebut hanya 17 fitur bobot tertinggi yang digunakan untuk melanjutkan proses klasifikasi *Naive Bayes Classifier.* Berikut fitur-fitur yang digunakan untuk Mendeteksi serangan DDoS dengan algoritma *Naive Bayes Classifier* :

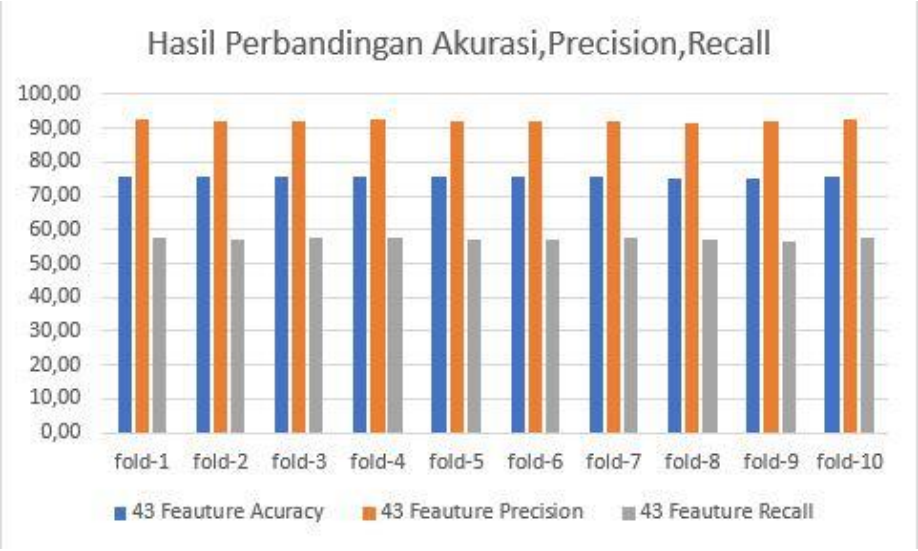
1 sttl
2 state
3 swin
4 dmean
5 dwin
6 ct_srv_src
7 ct_srv_dst
8 ct_dst_src_ltm
9 ct_dst_ltm
10 stcpb
11 ct_dst_sport_ltm
12 dtcpb
13 ct_src_dport_ltm
14 sjit
15 ct_src_ltm
16 is_sm_ips_ports
17 dttl

Dapat dilihat pada Gambar 5. bahwa klasifikasi kelas data “Normal” dan “Serangan” menggunakan metode *Naive Bayes Classifier* dengan dataset UNSW-NB15 menghasilkan akurasi yang cukup baik dengan metode *Cross validation* untuk teknik validasi model yang dilakukan dengan menilai hasil analisis secara akurat.

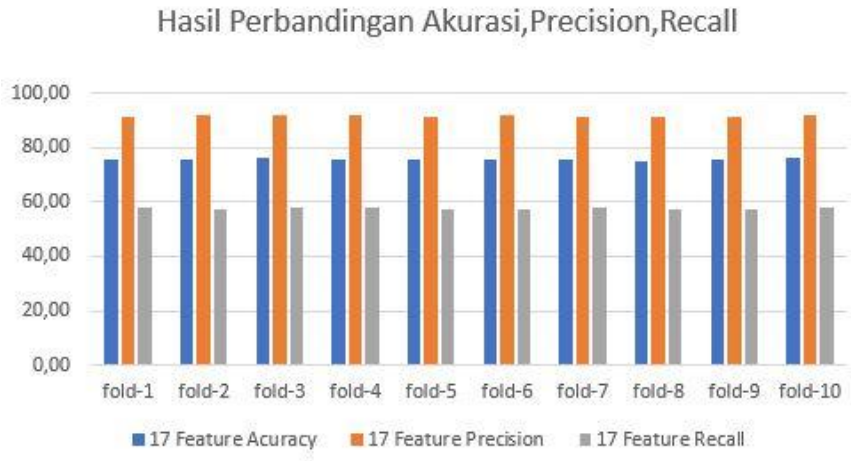
Hasil yang didapatkan oleh metode naive bayes classifier dengan penerapan seleksi fitur *information gain* menggunakan 17 fitur berdasarkan nilai entrophy tertinggi, memiliki rata-rata akurasi sebesar 75.81%. Sedangkan pengujian sistem klasifikasi *naive bayes classifier* tanpa penerapan seleksi fitur *information gain* mendapatkan hasil rata-rata akurasi sebesar 75.57%. Bahwa hasil perfoma sistem menggunakan 43 fitur UNSW-NB15 mendapatkan nilai rata-rata *precision* sebesar 92.20%. Selain menguji parameter *precision*,parameter *recall* juga akan di hitung berdasarkan *confusion matrix*.



Gambar 5. Grafik Hasil Rata-Rata Pengujian



Gambar 6. Grafik Hasil Performa Sistem 43 Fitur



Gambar 7. Grafik Hasil Performa Sistem 17 Fitur

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Untuk hasil nilai rata-rata *recall* didapatkan sebesar 57.31%. Pada hasil performa sistem menggunakan seleksi fitur *information gain* dengan 17 Fitur pada dataset UNSW-NB15, *precision* dan *recall* mendapatkan hasil yang sedikit berbeda dengan hasil performa menggunakan 43 fitur, tetapi untuk rata-rata hasil performa sistem menggunakan 17 fitur lebih unggul daripada performa sistem menggunakan 43 fitur. Hasil rata-rata *precision* sebesar 91.61% dan nilai rentang terendah terdapat pada fold-8 dengan nilai 91.15%, sedangkan nilai rentang tertinggi terdapat pada fold-4 dengan nilai 92.14%. Untuk hasil performa recall mendapatkan nilai rata-rata sebesar 57.63%, dan nilai rentang terendah terdapat pada fold-9 dengan nilai 57.03%, serta nilai rentang tertinggi terdapat pada fold-3 dengan nilai 58.27%.

Tabel 3. Hasil waktu eksekusi sistem menggunakan 17 fitur dan 43 fitur

Lama waktu eksekusi sistem dalam satuan detik	**17 Fitur**	**43 Fitur**
	89.17 detik	205.34 detik

Sistem juga mengukur lamanya waktu yang dibutuhkan untuk mengeksekusi program dalam hitungan detik. Waktu yang dibutuhkan untuk menjalankan program dengan 17 fitur lebih cepat dan efisien, 89.17 detik, sedangkan program dengan 43 fitur membutuhkan waktu lebih lama, 205.34 detik.

4. Kesimpulan

Hasil prediksi dengan metode klasifikasi *naive bayes classifier* akan memprediksi data normal dan serangan, jika prediksi *naive bayes* menyatakan normal terhadap data normal, maka hasil prediksi sama atau bisa dikatakan (*true)* dan jika prediksi *naive bayes* menyatakan serangan terhadap data normal, maka hasil prediksi tidak sama (*false*) begitu juga sebaliknya. Maka dari itu hasil prediksi klasifikasi dapat diukur dengan tingkat akurasi**,** *precision* dan *recall* berdasarkan *confusion matrix*.

Hasil skenario pengujian dilakukan pengujian sistem terhadap hasil perbandingan kinerja data yang sudah diseleksi fitur menggunakan 17 fitur dan tanpa penerapan seleksi fitur *information gain* menggunakan 43 fitur dengan metode 10 *Fold Cross Validation.* Hasil yang didapatkan lebih baik hasil penerapan seleksi fitur *Information Gain* dengan nilai rata-rata akurasi 75.81%,sedangkan hasil yang didapatkan tanpa penerapan seleksi fitur sebesar 75.57%. Sistem ini juga dapat mengeksekusi program dengan menggunakan 17 fitur lebih cepat dan efektif yaitu 89.17 detik, dibandingan dengan waktu eksekusi program yang menggunakan 43 fitur diperoleh waktu 205.34 detik.

Referensi

[1] D. B. Satmoko, P. Sukarno, and E. M. Jadied, “Peningkatan Akurasi Pendeteksian Serangan DDoS Menggunakan Multiclassifier Ensemble Learning dan Chi-Square Pendahuluan Studi Terkait,” vol. 5, no. 3, pp. 7977–7985, 2018.

[2] S. Anwar, F. Septian, and R. D. Septiana, “Klasifikasi Anomali Intrusion Detection System (IDS) Menggunakan Algoritma Naïve Bayes Classifier dan Correlation-Based Feature Selection,” *J. Teknol. Sist. Inf. dan Apl.*, vol. 2, no. 4, p. 135, 2019, doi: 10.32493/jtsi.v2i4.3453.

[3] K. Kurniabudi, A. Harris, and A. Rahim, “Seleksi Fitur Dengan Information Gain Untuk Meningkatkan Deteksi Serangan DDoS menggunakan Random Forest,” *Techno.Com*, vol. 19, no. 1, pp. 56–66, 2020, doi: 10.33633/tc.v19i1.2860.

[4] D. Pratama and S. S. Polytechnic, “SERANGAN DDOS PADA SOFTWARE-DEFINED NETWORK,” no. August 2019, 2021, doi: 10.31227/osf.io/a86cr.

[5] A. Fatkhurohman and E. Pujastuti, “Penerapan Algoritma Naïve Bayes Classifier untuk Meningkatkan Keamanan Data dari Website Phising,” *J. Teknol. Inf.*, vol. 15, no. 1, pp.

115–124, 2019.

[6] A. Prasetyo, L. Affandi, and D. Arpandi, “Implementasi Metode Naive Bayes Untuk Intrusion Detection System (Ids),” *J. Inform. Polinema*, vol. 4, no. 4, p. 280, 2018, doi: 10.33795/jip.v4i4.220.

[7] D. A. Nasution, H. H. Khotimah, and N. Chamidah, “Perbandingan Normalisasi Data untuk Klasifikasi Wine Menggunakan Algoritma K-NN,” *Comput. Eng. Sci. Syst. J.*, vol. 4, no. 1, p. 78, 2019, doi: 10.24114/cess.v4i1.11458.

[8] F. Tempola, M. Muhammad, and A. Khairan, “Perbandingan Klasifikasi Antara KNN dan Naive Bayes pada Penentuan Status Gunung Berapi dengan K-Fold Cross Validation,” *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 5, p. 577, 2018, doi: 10.25126/jtiik.201855983.