SISTEM DETEKSI INTRUSI MENGGUNAKAN ALGORITMA GENETIK PADA SERANGAN DOS DI PROTOKOL TCP DAN UDP

INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM ON DOS ATTACK IN TCP AND UDP PROTOCOL

Muhammad Akmal Fauzi[1], Ir. Ahmad Tri Hanuranto, M.T [2], Casi Setianingsih, S.T., M.T[3]

[1,2] Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

[3]Prodi S1 Sistem Komputer, Fakultas Teknik Elektro, Universitas Telkom

[1]**kemalemal90@gmail.com**, [2]**athanuranto@telkomuniversity.ac.id**, [3]**setiacasie@telkomuniversity.ac.id**

Abstrak

Pada saat ini perkembangan di dunia teknologi jaringan sangat pesat serta penggunaan internet yang semakin bertambah, dengan bertambahnya pengguna internet maka jumlah kebutuhan network pun juga ikut bertambah. Risiko dari bertambahnya jumlah kebutuhan network membuat lalu lintas jaringan semakin kompleks dan risiko penyerangan terhadap data yang dilindungi dari sebuah server.

Karena banyaknya ancaman yang terjadi di jaringan komputer, maka diperlukan sebuah sistem yang dapat mengamankan jaringan komputer tersebut. Intrusion Detection System atau yang biasa disebut dengan IDS adalah sistem yang memonitor lalu lintas jaringan untuk aktivitas yang mencurigakan dan memberikan peringatan ketika aktivitas tersebut ditemukan.

Untuk memecahkan masalah tersebut, pada Tugas Akhir ini dilakukan analisis dari proses IDS menggunakan KDD99 sebagai dataset dengan menggunakan algoritma genetik sebagai fitur seleksi dan algoritma KNN sebagai klasifikasi dan evaluasi. Berdasarkan pengujian yang dilakukan, fitur seleksi menggunakan algoritma genetik mendapatkan 18 fitur terbaik yang akan digunakan dari 41 fitur, dengan rata-rata akurasi 84,17 % , dan klasifikasi menggunakan algoritma KNN dengan akurasi data training 99,98%, data testing dengan rata-rata 97,52% dan rata-rata perhitungan manual diparameter k=1 78,57%, k=3 76,40%, k=5 76,86%, k=7 76,71%, k=9 77,57%.

Kata Kunci : *Intrusion Detection System, IDS, Genetic Akgorithm, GA, Security Network, Network Computer. K-NN, Dataset, KDD99.*

Abstract

At present the development in the world of network technology is very rapid and internet usage is increasing, with the increase in internet users, the number of network needs also increases. The risk of increasing the number of network needs makes network traffic more complex and the risk of attacking protected data from a server.

Because of the many threats that occur on computer networks, it requires a system that can secure the computer network. Intrusion Detection System or commonly called IDS is a system that monitors network traffic for suspicious activities and gives a warning when the activity is found.

To solve this problem, in this Final Project do analyze the IDS process using KDD99 as a dataset using genetic algorithms as a selection feature and KNN algorithm as classification and evaluation. Based on the tests performed, the selection feature uses a genetic algorithm to get the 18 best features to be used from 41 features, with an average accuracy of 84,17%, and classification using the KNN algorithm with accuracy of training data 99,98% , data testing with average 97,52% and the average manual calculation parameter k=1 78,57%, k=3 76,40%, k=5 76,86%, k=7 76,71%, k=9 77,57%.

Keywords **:** *: Intrusion Detection System, IDS, Genetic Akgorithm, GA, Security Network, Network Computer. K-NN, Dataset, KDD99..*

1. Pendahuluan

Pada saat ini perkembangan di dunia teknologi jaringan sangat pesat serta penggunaan internet yang semakin bertambah, dengan bertambahnya pengguna internet maka jumlah kebutuhan network pun juga ikut bertambah. Berbagai risiko dan ancaman terhadap aset yang tidak dikontrol dan tidak dilindungi seperti database dan web server dimana berguna untuk menyimpan data yang dapat diolah dan manipulasi menggunakan program aplikasi.

Ancaman pada jaringan komputer biasanya disebut dengan CyberAttacks merupakan serangan yang banyak digunakan dalam kejahatan, seperti mengambil dan mengubah data pribadi seseorang atau informasi dari kartu kredit pelanggan dan juga meretas situs web [1] dengan cara tersembunyi maupun terang-terangan.

Menurut penulis, banyaknya ancaman yang terjadi di jaringan komputer, maka diperlukan sebuah sistem yang dapat mengamankan jaringan komputer tersebut. Intrusion Detection System atau yang biasa disebut dengan IDS adalah sistem yang memonitor lalu lintas jaringan untuk aktivitas yang mencurigakan dan memberikan peringatan ketika aktivitas tersebut ditemukan [2]. IDS digunakan oleh Network Administrator untuk memantau kondisi jaringan, sehingga dapat mencegah terjadi serangan pada jaringan.

Berdasarkan ruang lingkup pendeteksianya, IDS terbagi menjadi 2 yaitu Network-Based IDS dan Host-Based IDS. Network-Based IDS adalah sebuah sistem yang berupaya menemukan akses ilegal ke jaringan komputer dengan menangkap paket trafik dan Host-Based IDS adalah Host yang melibatkan software atau komponen, yang memonitor prilaku dan keadaan sistem komputer [3]. Ada dua teknik pendeteksian pada IDS, yaitu signature based dan anomaly based. Pendeteksian signature based merupakan sistem pendeteksi yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap data signature based IDS yang bersangkutan. Sedangkan pada anomaly based merupakan suatu pendeteksi yang melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya pada pendeteksi tersebut biasanya dilakukan dengan menggunakan teknik statistik untuk membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. Metode ini menawarkan kelebihan dibandingkan signature-based IDS, dimana dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam data signature based IDS. Kelemahan pada pendeteksi ini adalah jenis ini sering mengeluarkan pesan false alarm. Sehingga tugas administrator menjadi lebih rumit, karena harus memilah jenis-jenis serangan yang sebenarnya dari banyaknya laporan false alarm yang muncul.

Pada penelitian sebelumnya, terdapat beberapa metode klasifikasi yang telah melakukan klasifikasi pada data IDS, seperti Support Vector Machine (SVM), Genetic Algorithm (GA), K-Nearest Neighbour (KNN), Artificial Neural Network (ANN), Bayesian Method, Decision Tree dan Fuzzy Logic [16]. Menurut [16], [18], dan [2] lambatnya waktu testing dan akurasi masih menjadi tantangan untuk penelitian mengenai metode klasifikasi pada IDS. IDS ini sudah banyak di teliti khususnya integrasi dengan Fuzzy-genetic Algorithm, J. Gómez and E. León dengan mengajukan Fuzzy-genetic Algorithm untuk mengkategorisasi aktifitas intrusi pada jaringan. Pada algoritma tersebut dapat mengkategorikan data menjadi DoS, R2L, Probe, U2R. [4]. Dalam realisasinya, Genetic Algorithm digunakan pada proses seleksi fitur yang dimana hasil seleksinya akan ditraining dan evaluated menggunakan metode KNN untuk klasifikasinya. Sehingga pada penulisan Tugas Akhir ini, IDS yang dilakukan menggunakan proses pengolahan data KDD yang dimana algoritma yang digunakan diterapkan pada proses seleksi fitur dan build model. Penelitian ini dilakukan untuk menguji performa metode KNN dalam klasifikasi data IDS dan Genetic Algorithm pada proses seleksi fitur, dengan membandingkan metode KNN dengan metode yang umum digunakan dalam klasifikasi. Diharapkan peneltian ini dapat menghasilkan tingkat akurasi yang baik dengan menguji parameter yang dapat mempengaruhi performa KNN.

2. Dasar Teori

2.1 Intrusion Detection System

Intrusion Detection System (IDS) adalah sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Intrusion Detection System (IDS) juga dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound pada sebuah sistem atau jaringan, dengan cara analisis dan mencari bukti dari percobaan intrusi (penyusupan).

Pada IDS terdapat sebuah pemberitahuan yang diberikan saat terjadinya intrusi yang masuk, pemberitahuan tersebut terbagi menjadi dua, yaitu true alarm dan false alarm. *True alarm* adalah saat intrusi sesungguhnya masuk kedalam jaringan. Sedangkan *False alarm* adalah saat IDS mendeteksi aktifitas yang bukan intrusi. Bila rasio deteksi tinggi dan false positive rendah, maka IDS tersebut terbilang baik [3].

2.2 Jenis Serangan Dalam Jaringan

Penyerangan dalam sistem jaringan dimana mempunyai keamanan yang canggih dan ketat pun masih memungkinkan sistem jaringan tersebut tak aman seratus persen dari penyalahgunaan sumber daya atau serangan

sistem jaringan para pencuri dunia maya. Berikut adalah macam-macam serangan pada sistem jaringan di *database* KDDCUP99:

2.2.1 DoS

Denial of Service (DoS) adalah serangan yang membuat sumber daya milik komputer atau server penuh dan tidak dapat memberikan pelayanan pada user sesungguhnya [3].

2.2.2 R2L

Remote to User attack (R2L) adalah serangan yang mana penyerang mengirimkan sebuah paket ke server atau komputer lain dimana dia tidak memiliki akses yang bertujuan untuk membuka kelemahan perangkat tersebut dan mengeksploitasi kewenangan user pada server atau komputer tersebut [3].

2.2.3 Probe

Probe adalah serangan dimana penyerang memindai perangkat untuk menentukan kelemahan yang dapat diekploitasi [3].

2.2.4 U2R

User to Root attack (U2R) penyerang akan masuk kedalam sistem dengan status sebagai user biasa lalu akan memanfaatkan kelemahan untuk membuka status administrator [3].

2.3 *Knowledge Discovery in Database* (KDD)

KDD adalah proses menentukan informasi yangberguna serta pola-pola yang ada dalam data. Informasi ini terkandung dalam basis data yang berukuran besar yang sebelumnya tidak diketahui dan potensial bermanfaat (Han &Kamber, 2006 dalam Baskoro, 2010).Pada proses *Knowledge Discovery Database (KDD)* terdapat beberapa fase yaitu : Seleksi Data (*Selection*), Pemilihan Data (*Preprocessing*/*Cleaning*), Transformasi (*Transformation*), *Data Mining* dan Interpretasi/Evaluasi (*Interpratation*/*Evaluation*). Pada fase terakhir ini yang dilakukan adalah proses pembentukan keluaran yang mudah dimengerti yang bersumber pada proses *Data Mining* Pola informasi. Dataset KDD Cup 99 adalah acuan data set yang awalnya digunakan didalam jaringan militer pada tahun 1998 lalu dinamakan menjadi KDD99 dengan 41 atribut pada tabel sebagai berikut [9].

Tabel I. Attribute KDD99

No.	Network attributes	No.	Network attributes	No.	Network attributes
1	duration	15	su_attempted	29	same_srv_rate
2	protocol_type	16	num_root	30	diff_srv_rate
3	service	17	num_file_creations	31	srv_diff_host_rate
4	flag	18	num_shells	32	dst_host_count
5	src_bytes	19	num_access_files	33	dst_host_srv_count
6	dst_bytes	20	num_outbound_cmds	34	dst_host_same_srv_rate
7	land	21	is_host_login	35	dst_host_diff_srv_rate
8	wrong_fragment	22	is_guest_login	36	dst_host_same_src_port_rate
9	urgent	23	count	37	dst_host_srv_diff_host_rate
10	hot	24	srv_count	38	dst_host_serror_rate
11	num_failed_logins	25	serror_rate	39	dst_host_srv_serror_rate
12	logged_in	26	srv_serror_rate	40	dst_host_rerror_rate
13	num_compromised	27	rerror_rate	41	dst_host_srv_rerror_rate
14	root_shell	28	srv_rerror_rate		

2.4 Algoritma *K-Nearest Neighbor*

K-Nearest Neighbor sering digunakan dalam klasifikasi dengan tujuan dari algoritma ini adalah untuk mengklasifikasi objek baru berdasarkan atribut dan training samples. Algoritma *K-Nearest Neighbor* (K-ANN atau KNN) adalah sebuah metode untuk melakukan klasifikasi terhadap objek berdasarkan data pembelajaran yang jaraknya paling dekat dengan objek tersebut. Teknik ini sangat sederhana dan mudah diimplementasikan. Data pembelajaran diproyeksikan ke ruang berdimensi banyak, dimana masing-masing dimensi merepresentasikan fitur dari data. Ruang ini dibagi menjadi bagian-bagian berdasarkan klasifikasi data pembelajaran. Sebuah titik pada ruang ini ditandai kelas c jika kelas c merupakan klasifikasi yang paling banyak ditemui pada k buah tetangga terdekat titk tersebut. Dekat atau jauhnya tetangga biasanya dihitung berdasarkan jarak Euclidean [22]. Untuk mendefinisikan jarak antara dua titik yaitu titik pada data training (x) dan titik pada data testing (y) maka digunakan rumus Euclidean sebagai berikut.

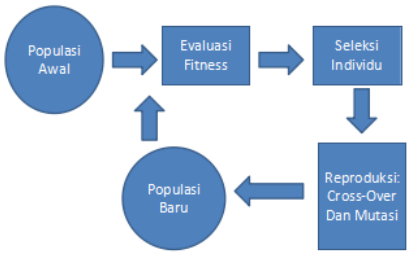
$$d(x,y) = \sqrt{\sum_{i=1}^{n} f((Xi:Yi) - (Wi)^2} \quad (1)$$

Keterangan :

- x=data training
- y=data testing
- n=Jumlah atribut
- f =fungsi similiarity antara titik x dan titik y
- wi=bobot yang diberikan pada atribut i

2.5 *Genetic Algorithm*

Genetic Algorithm (GA) merupakan salah satu bagian dari algoritma evolusioner, yaitu algoritma yang mengikuti prinsip reproduksi dan seleksi alam dari teori evolusi Darwin [24]. Dalam proses evolusi, individu secara terus menerus mengalami perubahan gen untuk menyesuaikan dengan lingkungan hidupnya. Dan proses seleksi alamiah ini melibatkan perubahan gen yang terjadi pada individu melalui proses perkembang-biakan, dimana proses ini menjadi proses dasar dengan pola pikir : "Bagaimana cara mendapatkan keturunan yang lebih baik". Di dalam algoritma genetik ini juga melibatkan operasi genetika seperti *crossover* dan *mutation* untuk mendapatkan individu terbaik.

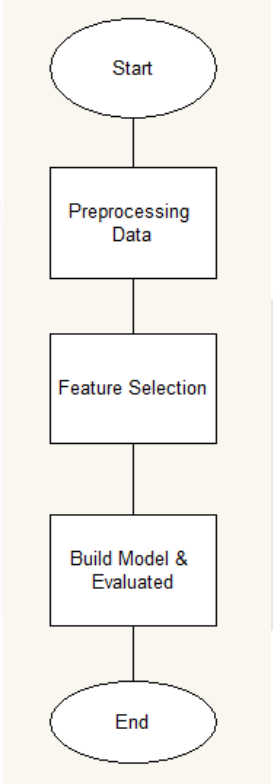


Gambar I. Diagram proses algoritma genetik

3. Perancangan Sistem

Diagram Alir Perancangan

Pembuatan Tugas Akhir ini dikerjakan dengan melakukan perancangan dan langkah-langkah awal perancangan sampai dengan analisis akhir sesuai Gambar 3.1 dibawah ini.



Gambar II. Diagram Alir Perancangan

Perancangan dan langkah-langkah pengerjaan tigas akhir seperti pada Gambar 3.1 adalah sebagai berikut. Pertama yaitu melakukan *preprocessing* data dari data yang sudah di unduh dalam bentuk file dimana pada data *train* menggunakan dataset " *kddcup.data_10_percent_corrected*" dan *test* menggunakan dataset "*corrected*" dimana *output* dari *preprocessing* dataset yang telah diberikan nama atribut pada setiap kolom berbentuk file CSV, setelah data sudah dilakukan *preprocessing* langkah yang kedua adalah melakukan seleksi fitur, dimana pada proses ini menggunakan algoritma genetik yang akan menseleksi dari 41 fitur dataset KDD99 menjadi beberapa fitur yang selanjutnya fitur tersebut akan dilakukan *Build Model & Evaluated* ,pada tahap ini proses yang dilakukan menggunakan algoritma KNN.

.

4. Hasil Pengujian dan Analisis

4.1 Skenario Pengujian

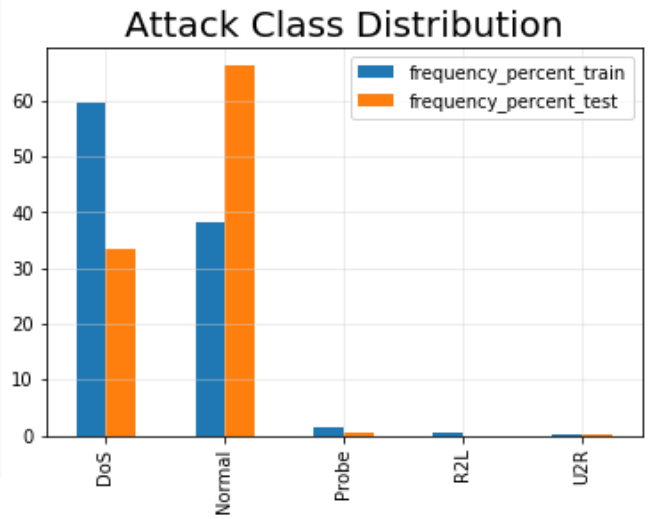
Skenario pengujian dilakukan dari mendapatkan dataset, pengolahan data, seleksi fitur, *build model* dan evaluasi. Dataset yang diperoleh dari situs KDD99 [28] dengan dataset untuk *training* menggunakan dataset "*kddcup.data_10_percent_corrected*" yang telah dikurangi 3% dari data aslinya, sedangkan untuk data *training* menggunakan dataset "*corrected*". Setelah data didapat adapun proses pengujianya dibagi dalam beberapa tahap berikut.

a) Preprocessing

Pada proses ini, setelah dataset didapat kemudian dilakukanlah proses *preprocessing* dan pembersihan data yang merupakan operasi dasar seperti penghapusan noise dilakukan. Sebelum proses data *mining* dapat dilaksanakan, perlu dilakukan proses *cleaning* pada data yang menjadi fokus KDD. Proses *cleaning* mencakup antara lain membuang duplikasi data, memeriksa data yang *inkonsisten*, dan memperbaiki kesalahan pada data, seperti kesalahan cetak (*tipografi*). Pada proses ini juga data akan dikelompokan berdasarkan dari tipe data tersebut.

	attack_class	frequency_percent_train	attack_class	frequency_percent_test
DoS	148931	59.57	5000.0	33.34
Normal	95906	38.36	9936.0	66.24
Probe	3989	1.60	59.0	0.39
R2L	1126	0.45	NaN	NaN
U2R	48	0.02	4.0	0.03

Gambar III. Jumlah data terklasifikasi



Gambar IV. *Attack Class Distribution*

b) Selection Feature

Proses *feature selection* ini menggunakan algoritma genetik, dengan parameter yang diuji adalah akurasi, *recall, precission* dan nilai fitness dengan rumus yang digunakan

$$Akurasi = \frac{(TP+TN)}{(TP+TN+FP+FN)} \quad (2)$$

$$Precission = \frac{TP}{(TP+FP)} \quad (3)$$

$$Recall = \frac{TP}{(TP+FN)} \quad (4)$$

$$Fitness = 60\%\ Akurasi + 20\%\ Recall + 20\%\ Precission \quad (5)$$

Pada proses GA ini yang akan menseleksi fitur-fitur yang akan dievaluasi, dari 41 fitur yang nantinya akan dipilih fitur mana yang terbaik untuk dilakukanya evaluasi dengan populasi = 20, *crossover* = 0.15 dan *mutation* = 0.1.

c) Build model and evaluated

Pada tahap ini adalah pengujian data *training* dan *testing* setelah dilakukanya seleksi fitur yang didapat dengan menggunakan algoritma K-NN untuk klasifikasi. Evaluasi yang dilakukan mencari akurasi dan deteksi pada kalsifiakasi data normal dan DoS untuk mencari nilai kebenaran dari data *testing* dan *training* dalam keluaran berupa *confusion matrix* dengan pengujian baik dari dataset *testing* dan juga data *sampling* secara manual dengan parameter k=1, 3, 5, 7 dan 9.

4.2 Hasil Pengujian

a) Hasil *feature selection*

Hasil dari seleksi fitur ini berupa parameter yang sudah dijelaskan pada scenario pengujian dan juga berupa grafik, dengan hasil :

Tabel II. Hasil parameter *feature selection*

Akurasi	80.215 %
Precission	90.069 %
Recall	90.147 %
Fitnes	84.171 %

Tabel III. Hasil *feature selection* yang akan digunakan.

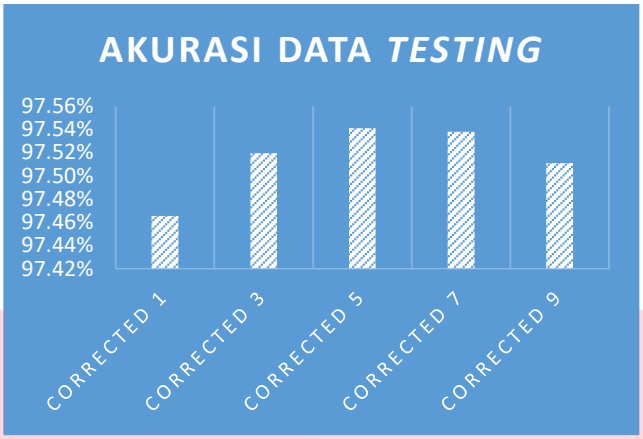
Fitur yang terseleksi	
service	srv_count
flag	rerror_rate
src_bytes	srv_rerror_rate
land	same_srv_rate
num_root	diff_srv_rate
num_shells	srv_diff_host_rate
is_host_login	dst_host_same_src_port_rate
is_guest_login	dst_host_serror_rate
count	dst_host_rerror_rate

b) Hasil Klasifikasi

Hasil dari klasifikasi menggunakan algoritma K-NN pada *trainig* set dengan akurasi sebesar 99.95% dan untuk *testing* set mendapatkan rata-rata akurasi sebesar 97.52% yang diperoleh dari rumus akurasi.

Tabel IV. Hasil *training* data

Data *Training*		
	DoS	Normal
DoS	391398	60
Normal	12	191446
Akurasi	99.98%	
Cross Validasi	99.29%	



Gambar 5. Hasil *testing* data

Hasil setiap pengujian data diatas terhadap metode KNN dapat dijelaskan pada tabel berikut.

Tabel V. Hasil *testing* data *corrected*

No	Parameter	DoS		Normal		Akurasi
		TN	FP	FN	TP	
1	K=1	223377	6476	885	59708	97.47%
2	K=3	223539	6314	890	59703	97.52%
3	K=5	223507	6346	796	59797	97.54%
4	K=7	223504	6349	802	59791	97.54%
5	K=9	223432	6421	808	59785	97.51%
Rata-Rata Akurasi						97.52%

Dari hasil analisis menggunakan dataset *corrected* didapat dengan rata-rata akurasi sebesar 97.52% dengan menggunakan parameter k=1,3,5,7, dan 9. Dan parameter yang memiliki tingkat akurasi terbaik dengan nilai akurasi sebesar 97.54% pada parameter K=5 dan K=7.
Kemudian hasil analisis manual dengan sampel data 1000, 5000, 10000, 15000 dan 30000 pada klasifikasi DoS dan Normal data dengan hasil sebagai berikut.

Tabel VI. Hasil *testing* data manual parameter k=1,3,5,7, dan 9

No	Parameter K	Data Pengujian	DoS		Normal		Akurasi	Rata-rata akurasi
			TN	FP	FN	TP		
1	K=1	1000	304	724	37	935	61.95%	78.57%
		5000	2341	2659	248	9688	80.54%	
		10000	6655	3345	4	4992	77.67%	
		15000	11595	3405	4	4992	82.95%	
		30000	26422	3578	4	4992	89.76%	
2	K=3	1000	273	755	282	690	48.15%	76.40%
		5000	2372	2628	255	9681	80.70%	
		10000	6598	3402	4	4992	77.29%	
		15000	12171	2829	4	4992	85.83%	
		30000	26512	3488	2	4994	90.03%	
3	K=5	1000	700	328	669	303	50.15%	76.86%
		5000	2453	2547	282	9654	81.06%	
		10000	6653	3347	3	4993	77.66%	
		15000	11641	3359	3	4993	83.19%	
		30000	36508	3492	2	4994	92.23%	
4	K=7	1000	749	279	695	277	51.30%	76.71%
		5000	2590	2410	284	9652	81.96%	
		10000	6593	3407	3	4993	77.26%	
		15000	11606	3394	3	4993	83.01%	
		30000	26509	3491	2	4994	90.02%	
5	K=9	1000	869	159	729	249	55.73%	77.57%
		5000	2564	2436	285	9651	81.78%	
		10000	6592	3408	3	4993	77.25%	
		15000	11617	3383	3	4993	83.07%	
		30000	26506	3494	0	4996	90.02%	

5. Kesimpulan

Berdasarkan hasil desain perancangan, realisasi, dan pengujian dapat dihasilkan beberapa kesimpulan antara lain yaitu:

1. Hasil yang didapat dari seleksi fitur menggunakan algoritma genetik adalah dengan nilai fitness 84.171% dan fitur yang terseleksi berjumlah 18 dari 41 fitur yang ada.
2. Hasil dari evaluasi pengujian menggunakan algoritma K-NN untuk data *training* dengan akurasi sebesar 99.98% dan untuk data *testing* sebesar 97.54% pada parameter k=5 dan k=7 dengan rata-rata akurasi 97.52%.
3. Hasil akurasi dari pengujian manual pada evaluasi di k=1,3,5,7 dan 9 dari 1000, 5000, 10000, 15000, dan 30000 dengan rata-rata tingkat akurasi sebesar 78.57%, 76.40%, 76.86%, 76.71%, dan 77.57%. Pada parameter tersebut memiliki tingkat akurasi tertinggi sebesar 78.57% pada parameter k=1 dan tingkat akurasi terendah dengan akurasi sebesar 76.40% pada parameter K=3.

Beberapa pertimbangan yang dapat diperhatikan untuk penelitian selanjutnya. Pertimbangan-pertimbangan tersebut antara lain seperti:

1. Dalam pelekukan *feature selection* menggunakan algoritma genetik sebaiknya fitur seleksinya diuji beberapa sample dan diambil nilai fitness yang paling bagus.
2. Data yang digunakan untuk pengujian sebaiknya menggunakan lebih dari 1 jenis dataset untuk IDS yang telah tersedia.
3. Pemilihan dataset sebaiknya dicocokan pada aplikasi dan perangkat yang akan digunakan dalam pengujian.
4. Untuk penelitian selanjutnya pada proses fitur seleksi dan evaluasi dibandingkan dengan algoritma lain, untuk mendapatkan hasil yang optimal kedepanya

Daftar Pustaka:

[1] W. H. Boothby, W. H. Von Heinegg, J. B. Michael, M. N. Schmitt, and T. C. Wingfield, "*When is a cyberattack a use of force or an armed attack?*," *Computer (Long. Beach. Calif).*, vol. 45, no. 8, pp. 82–84, 2012.

[2] S. E. Benaicha, L. Saoudi, S. E. B. Guermeche, and O. Lounis, "Intrusion detection system using genetic algorithm," *2014 Sci. Inf. Conf.*, vol. 00, no. c, pp. 564–568, 2014.

[3] S. Potteti and N. Parati, "Intrusion detection system using hybrid Fuzzy Genetic algorithm," *Proc. - Int. Conf. Trends Electron. Informatics, ICEI 2017*, vol. 2018–Janua, pp. 613–618, 2018.

[4] P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo "*Real-Time Intrusion Detection with Fuzzy Genetic Algorithm*." ©2013 IEEE

[5] S. Bharath Reddy, D. Malathi, and S. Jose, "An intrusion detection and prevention system in cloud computing: A technical review," ARPN J. Eng. Appl. Sci., vol. 12, no. 12, pp. 3723–3729, 2017.

[6] E.-F. Geoffroy, G. (George) Douglas, W. Innys, R. Manby, and T. Woodward, "A treatise of the fossil, vegetable, and animal substances, that are made use of in physick. : Containing the history and description of them; with an account of their several virtues and preparations. To which is prefixed, an enquiry into the constituent," vol. 28, no. 7, pp. 26–35, 2011.

[7] D. P. Bratu, B.-J. Cha, M. M. Mhlanga, F. R. Kramer, and S. Tyagi, "Visualizing the distribution and transport of mRNAs in living cells," *Proc. Natl. Acad. Sci.*, vol. 100, no. 23, pp. 13308–13313, 2003.

[8] A. P. Plerou, "Fuzzy Genetic Algorithms : Fuzzy Logic Controllers and Genetics Algorithms Original Research Paper Commerce Engineering Fuzzy Genetic Algorithms : Fuzzy Logic Controllers and Genetics Algorithms Antonia Plerou Elena Vlamou Vasil Papadopoulos Department of," no. November 2016, 2017.

[9] Jun-Zhong Zhao, & Hou-Kuan Huang. (n.d.), (2002). *An intrusion detection system based on data mining and immune principles*. Proceedings. International Conference on Machine Learning and Cybernetics.

[10] Improved Genetic Algorithm for Intrusion Detection System. 2014 International Conference on Computational Intelligence and Communication Networks

[11] V. Moraveji Hashemi, Z. Muda and W. Yassin, (2013). *Improving Intrusion Detection Using Genetic Algorithm*. Information Technology Journal, 12: 2167-2173.

[12] Mehmood, T., & Rais, H. B. M. (2016). Machine learning algorithms in context of intrusion detection

[13] Danane, Y., & Parvat, T. (2015). Intrusion detection system using fuzzy genetic algorithm

[14] Senthilnayaki, B., Venkatalakshmi, K., & Kannan, A. (2015). Intrusion detection using optimal genetic feature selection and SVM based classifier

[15] Nursalim, S., and Himawan, H. *Klasifikasi bidang kerja lulusan meng- gunakan algoritma k-nearest neighbor*. Jurnal Tekonologi Informasi 10 , 1 (2014), 31–43

[16] Religia, Y. Feature extraction untuk klasifikasi pengenalan wajah meng- gunakan support vector machine dan k-nearest neighbor.

[17] Matthew Walker, Introduction to Genetic Programming, 2001

[18] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[19] Z. Kermansavari, H. Jazayeriy dan S. Fateri, Intrusion Detection System In Computer Network Using Decision Tree and SVM Algorithm

[20] Rahmani, Rasoul & Chizari, Milad & Eslami, Mohammad & Aslahi, Masi & Maralani, A & Golkar, Mohammad Javad & Ebrahimi, A. (2015). *A hybrid method consisting of GA and SVM for intrusion detection system. Neural Computing and Applications*. 27. 10.1007/500521.

[21] Saleh, A. I., Talaat, F. M., & Labib, L. M. (2017). A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifier.