

**ANALISIS ANOMALY BOTNET DENGAN METODE K-NN (K-
Nearest Neighbor)**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika



diajukan oleh

HAJAR DEWANTORO DJARI

17.11.1685

Kepada

PROGRAM SARJANA

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

**ANALISIS ANOMALY BOTNET DENGAN METODE K-NN (K-
Nearest Neighbor)**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



diajukan oleh

HAJAR DEWANTORO DJARI

17.11.1685

Kepada

PROGRAM SARJANA

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN

**ANALISIS ANOMALY BOTNET DENGAN METODE K-NN (K-
Nearest Neighbor)**

SKRIPSI

yang disusun dan diajukan oleh

Hajar Dewantoro Djari

17.11.1685

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 17 September 2022

Dosen Pembimbing

Sudarmawan, S.T, M.T

NIK. 190302035

HALAMAN PENGESAHAN

SKRIPSI

**ANALISIS ANOMALY BOTNET DENGAN METODE K-NN (K-
Nearest Neighbor)**

yang disusun dan diajukan oleh

Hajar Dewantoro Djari

17.11.1685

Telah dipertahankan di depan Dewan Penguji
pada tanggal 17 September 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Banu Santoso, S.T, M.En

NIK. 190302327

Windha Mega Pradnya D, M.Kom

NIK. 190302185

Subektiningsih, M.Kom

NIK. 190302413

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 17 September 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom.

NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Hajar Dewantoro
DjariNIM : 17.11.1685

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS ANOMALY BOTNET DENGAN METODE K-NN

(K- *Nearest Neighbor*)

Dosen Pembimbing : Sudarmawan, S.T, M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 17 September 2022 Yang Menyatakan,



Hajar Dewantoro Djari

HALAMAN PERSEMBAHAN

Alhamdulillah penulis mengucapkan banyak terima kasih dan rasa syukur kepada Allah SWT yang telah memberikan petunjuk dalam proses menyelesaikan penulisan skripsi ini. Dengan kerendahan hati, skripsi ini penulis persembahkan kepada:

1. Kedua Orang Tua yang saya sayangi Bapak Ondong Djari dan Ibu Marwiyah Toladi yang senantiasa selalu mensupport, mendo'akan saya dan selalu menasehati saya di kala saya lalai dalam mengerjakan skripsi.
2. Orang- orang terkasih Putri Tunggal Ramadhan W, Reiga Vangelo, Sukardi Sulang, dan Sulasmi Djari
3. Almamater tercinta "Universitas Amikom"



KATA PENGANTAR

Assalamu'alaikum warahmutullahi wabarakatu,

Puji syukur atas kehadiran Allah Subhanahu Wa Ta'ala yang telah memberikan rahmat dan hidayah-Nya sehingga peneliti dapat menyelesaikan skripsi yang berjudul “ANALISIS ANOMALY BOTNET DENGAN METODE K-NN (K- *Nearest Neighbor*)” dengan baik. Skripsi ini disusun sebagai salah satu persyaratan untuk mencapai derajat Sarjana Informatika Fakultas Ilmu Komputer Universitas Amikom Yogyakarta. Penyelesaian skripsi ini tidak lepas dari bimbingan dan dukungan dari berbagai pihak. Oleh karena itu penulis ingin mengucapkan terima kasih kepada:

1. Bapak M. Suyanto, Prof. Dr, M.M., selaku rektor Universitas Amikom Yogyakarta.
2. Ibu Krisnawati, S.Si., M.T., selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Sudarmawan, M.T., selaku ketua program studi Informatika sekaligus dosen pembimbing.
4. Tim penguji, segenap dosen dan karyawan Universitas Amikom Yogyakarta yang telah memberikan ilmu pengetahuan dan dukungan moral.

Semoga amal kebaikan dari semua pihak di atas mendapatkan imbalan yang berlipat dari Allah SWT dan atas semuanya semoga menjadi barokah. Aamiin

Penulis menyadari bahwa penyusunan skripsi ini masih jauh dari kata sempurna sehingga segala saran dan kritik yang bersifat membangun sangat diharapkan oleh penulis. Semoga skripsi ini dapat bermanfaat bagi ilmu pengetahuan pada umumnya dan semoga ilmu yang penulis peroleh mendapat keberkahan dari Allah SWT.

Wassalamualaikum Warahmatullahi Wabarakatuh.

Yogyakarta, 17 September 2022

Penulis

DAFTAR ISI

HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	v
HALAMAN PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xi
INTISARI.....	xii
ABSTACT.....	xiii
BAB I PENDAHULUAN	
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	2
1.3. Batasan Masalah.....	3
1.4. Maksud dan Yujuan Penulisan.....	3
1.5. Manfaat Penelitian.....	3
1.6. Metode Penelitian.....	4
1.7. Sistematika Penulisan.....	4
BAB II LANDASAN TEORI	
2.1. Kajian Pustaka.....	6
2.2. Kajian Teori.....	13

a. Metode K-Nearest Neighbor.....	13
b. Botnet.....	15

BAB III

METODE PENELITIAN

3.1. Gambaran Umum	16
3.2. Fase Requirement Analisis	17
3.2.1. Instalasi Perangkat Lunak.....	18

BAB IV

HASIL DAN PEMBAHASAN

4.1. Fase Implementasi	23
4.1.1. Import Library.....	23
4.1.2. Ambil Data.....	25
4.2.3. Penerapan Code K-NN dengan K=2.....	28
5.1. Kesimpulan.....	32
5.2. Saran	33

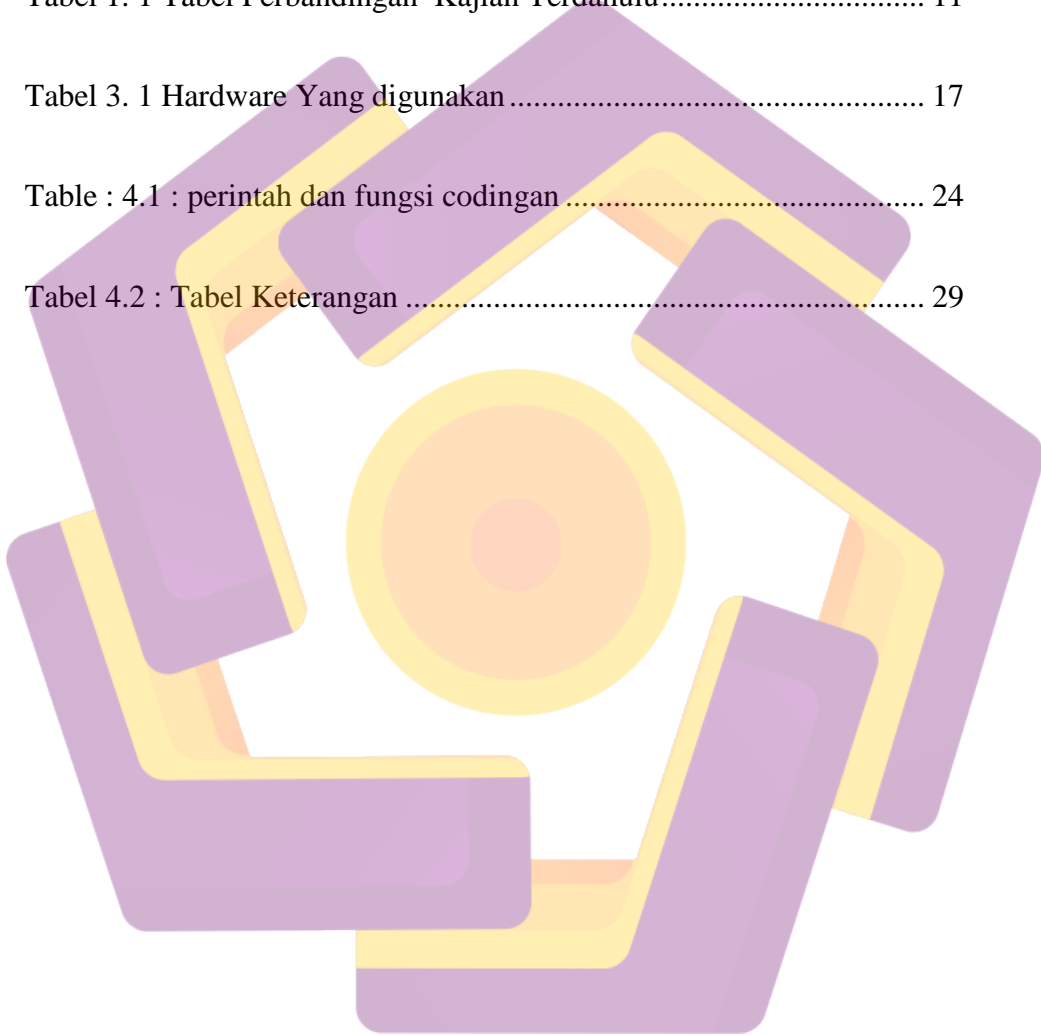
DAFTAR PUSTAKA.....	34
---------------------	----

DAFTAR GAMBAR

Gambar 2.1 K-Nearest Neighbor.....	14
Gambar 3.1 : Flowchart K-NN.....	16
Gambar 3.2.1 : proses instalasi python.....	18
Gambar 3.2.2 : Instalasi Jupyter Python.....	19
Gambar 3.2.3 : Instalasi Jupyter Notebook	20
Gambar 3.2.4 : Instalasi Pandas-numpy	21
Gambar 3.2.5 : Instalasi Sklearn.model.....	21
Gambar : 3.10 Dataset Anomaly	22
Gambar : 4.1.1 Perintah Import Library.....	24
Gambar : 4.1.2 Ambil data.....	26
Gambar : 4.1.3 Inputan data	27
Gambar 4.1.4 : x_train.....	29
Gambar 4.1.5: Hasil Penyebaran Anomaly	30
Gambar 4.1.6 : Sklearn.model Tree.....	31

DAFTAR TABEL

Tabel 1. 1 Tabel Perbandingan Kajian Terdahulu.....	11
Tabel 3. 1 Hardware Yang digunakan.....	17
Table : 4.1 : perintah dan fungsi codingan.....	24
Tabel 4.2 : Tabel Keterangan	29



INTISARI

Perkembangan di dunia internet saat ini mengalami kemajuan yang sangat pesat salah satunya di dunia jaringan komputer dan internet sehingga memicu pengguna internet yang semakin banyak, Hal ini menyebabkan Masalah – masalah baru yang bermunculan seperti serangan dan ancaman bagi pengguna internet saat ini. Ada berbagai macam serangan yang dimaksudkan untuk mencuri data dan informasi penting dan berharga untuk di salah gunakan demi kepentingan pribadi. Botnet adalah salah satu malware yang memiliki ancaman serius bagi keamanan internet. Dikarenakan botnet mampu melakukan serangan ilegal yakni *spam*, *phishing*, *klik faund*, pencurian password dan *distributed denial of serfice (DDoS) attack*.

Tujuan dari penelitian ini adalah Mendeteksi botnet pada jaringan peer to peer dengan menggunakan metode K-NN, Membedakan jaringan yang sah dan tidak sah pada jaringan peer to peer dengan K-NN dan Memberikan edukasi untuk selalu waswpada akan adanya serangan pada jaringan yang digunakan. Adapun metode yang digunakan yaitu metode *K-Nearest Neighbor* adalah algoritma untuk mengklasifikasi objek baru berdasarkan atribut dan training samples (data latih). Adapun model peneliatian yang digunakan dalam penulisan ini ialah ujicoba apakah KNN dapat mendeteksi botnet secara akurat.

berdasarkan hasil penelitian yang di implementasikan dari pengujian yang telah dilakukan Bahwa KNN mampu mendeteksi anomaly pada jaringan dengan akurasi bisa mencapai 95,6%. Untuk menyempurnakan dan mengembangkan penelitian yang peneliti lakukan maka peneliti memiliki beberapa saran yang perlu di sesuaikan dengan penelitian berikutnya yaitu bisa menentukan dengan baik system operasi yang digunakan yang familiar dan selaras dengan tools yang nantinya digunakan.

Kata kunci: Botnet, metode K-Nearest Neighbor (KNN), Anomaly

ABSTRACT

Developments in the internet world are currently experiencing very rapid progress, one of which is in the world of computer networks and the internet, thus triggering more and more internet users, this causes new problems to emerge such as attacks and threats to internet users today. There are various kinds of attacks that are intended to steal important and valuable data and information to be misused for personal gain. Botnet is one of the malware that poses a serious threat to internet security. Because botnets are capable of carrying out illegal attacks, namely spam, phishing, click fraud, password theft and distributed denial of service (DDoS) attacks.

The purpose of this study is to detect botnets on peer to peer networks using the K-NN method, to distinguish legitimate and unauthorized networks from peer to peer networks with K-NN and to provide education to always be aware of attacks on the network used. The method used is the K-Nearest Neighbor method, which is an algorithm for classifying new objects based on attributes and training samples (training data). The research model used in this paper is a test of whether KNN can detect botnets accurately.

based on the results of the research implemented from the tests that have been carried out that KNN is able to detect anomalies in the network with an accuracy that can reach 95.6%. To perfect and develop the research that the researcher is doing, the researcher has several suggestions that need to be adjusted to the next research, namely being able to properly determine the operating system used which is familiar and in harmony with the tools that will be used later.

Keywords: Botnet, K-Nearest Neighbor (KNN) method, Anomaly

