DETEKSI & KLASIFIKASI SERANGAN DDOS MENGGUNAKAN ALGORITMA KNN, NAÏVE BAIYES, STOCHASTIC GRADIENT DESCENT, DAN XGBOOST

(Studi Kasus: CV. Hardi Junior)

SKRIPSI

Disusun oleh:

Hartoyo Wahyu Setiadi
18.83.0232

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2021

DETEKSI & KLASIFIKASI SERANGAN DDOS MENGGUNAKAN ALGORITMA KNN, NAÏVE BAIYES, STOCHASTIC GRADIENT DESCENT, DAN XGBOOST

(Studi Kasus: CV. Hardi Junior)

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer

Disusun oleh:

Hartoyo Wahyu Setiadi
18.83.0232

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

HALAMAN PERSETUJUAN

SKRIPSI

DETEKSI & KLASIFIKASI SERANGAN DDOS MENGGUNAKAN ALGORITMA KNN, NAÏVE BAIYES, STOCHASTIC GRADIENT DESCENT, DAN XGBOOST PADA CV. HARDI JUNIOR

yang dipersiapkan dan disusun oleh

Hartoyo Wahyu Setiadi

18.83.0232

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 Desember 2021

Dosen Pembimbing,

Dony Artyus, M.Kom
NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI & KLASIFIKASI SERANGAN DDOS MENGGUNAKAN ALGORTIMA KNN, NAÏVE BAIYES, STOCHASTIC GRADIENT DESCENT, DAN XGBOOST PADA CV. HARDI JUNIOR

yang dipersiapkan dan disusun oleh

Hartoyo Wahyu Setiadi

18.83.0232

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Februari 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Muhammad Koprawi, S.Kom., M.Eng **NIK. 190302454**	
Wahid Miftahul Ashari, S.Kom., M.T **NIK. 190302452**	
Dony Ariyus, M.Kom **NIK. 190302128**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 25 Februari 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Hartoyo Wahyu Setiadi
NIM : 18.83.0232

Menyatakan bahwa Skripsi dengan judul berikut:

Deteksi & Klasifikasi Serangan DDoS Menggunakan Algoritma KNN, Naïve Bayes, Stochastic Gradient Descent, dan XGBoost pada CV. Hardi Junior

Dosen Pembimbing : Dony Ariyus, M.Kom

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, 21 Februari 2022

Yang Menyatakan,

Hartoyo Wahyu Setiadi

HALAMAN MOTTO

"Teruslah Mengocok Patrick"

(*Spongebob Squarepants*)

HALAMAN PERSEMBAHAN

Dengan rasa syukur yang mandalam, dengan telah diselesaikannya sektipsi ini penulis mempersembahkan kepada :

1. Keluarga besar Penulis yang telah senantiasa membantu menyelesaikan Skripsi ini.
2. Segenap *civitas* akademika kampus Universitas Amikom Yogyakarta, staf pengajar, karyawan dan seluruh mahasiswa semoga tetap semangat dalam beraktivitas mengisi hari-harinya di kampus Universitas Amikom Yogyakarta.
3. Teman-teman Penulis baik itu teman kuliah seangkatan, adik kelas, kakak kelas pada Fakultas Ilmu Komputer khususnya Program Studi Teknik Komputer yang telah banyak memberi masukkan, semangat, dan arahan hingga akhirnya dapat terselesaikan Skripsi ini.

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadirat Allah SWT, karena berkat rahmat dan karunia – Nya, penulis dapat menyelesaikan skripsi yang berjudul "Deteksi & Klasifikasi Serangan DDoS Menggunakan Algoritma KNN, Naïve Bayes, Stochastic Gradient Descent dan XGBoost pada CV. Hardi Junior".

Penulis menyadari bahwa dalam penulisan skripsi ini tidak lepas dari kesalahan dan jauh dari sempurna. Untu kitu penulis mengharapkan kritik dan saran yang bersifat membangun sehingga dapat beguna baik bagi penulisa sendiri maupun pembaca pada umumnya.

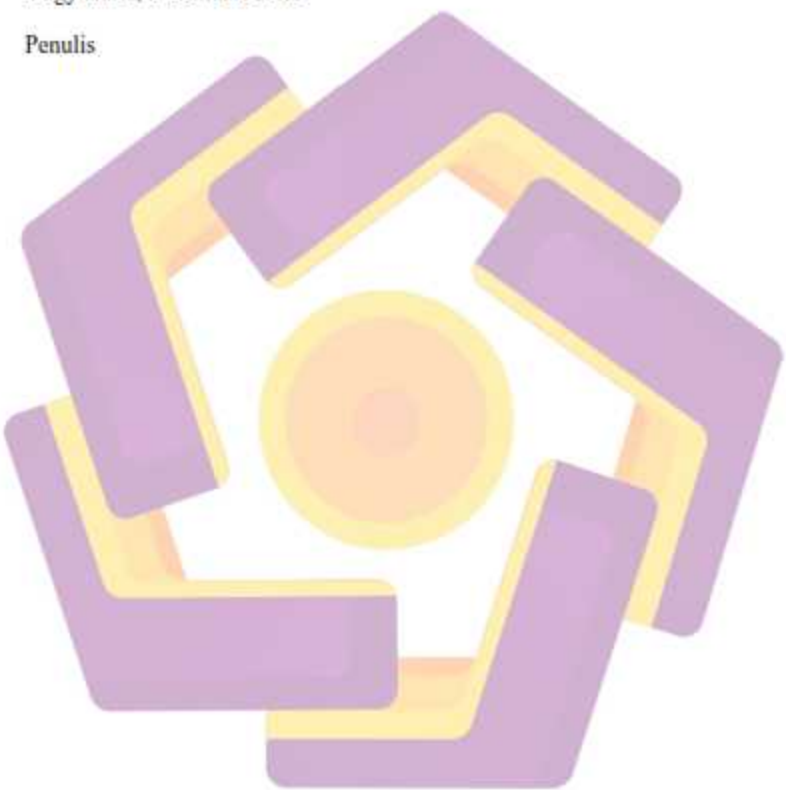
Dalam menyelesaikan skripsi ini, penulis telah banyak mendapatkan bantuan serta dukungan, baik secara moril maupun materil. Untuk itu dalam kesempatan ini penulis menyampaikan ucapan terima kasih kepada:

1. Dony Ariyus, M.Kom, selaku Kepala Program Studi Teknik Komputer sekaligus dosen pembimbing yang telah sabar meluangkan waktu, tenaga, dan pikirannya untuk membimbing dan mengarahkan penulis dalam menyelesaikan skripsi ini.
2. Bapak dan Ibu dosen Program Studi Teknik Komputer yang telah memberikan ilmunya kepada penulis, semoga Bapak dan Ibu dosen selalu diberikan ramah dan lindungan Allah SWT. Sehinnga ilmu yang telah diajarkan dapat bermanfaat dikemudian hari.
3. Ungkapan terima kasih dan penghargaan yang sangat spesial penulis haturkan dengan rendah hati kepada kedua orang tua penulis yang tercinta, Ayahanda Suharno, ST dan Ibunda Rochani serta kakak dan adik penulis yang dengan segala pengorbanannya tak akan pernah penulis lupakan atas jasa-jasa mereka.

4. Fauzan Alfiansyah Tasty, selaku sahabat yang telah membantu meminjamkan perangkatnya sehingga penulis dapat menyusun dan menyelesaikan skripsi dengan baik.

Yogyakarta, 26 Januari 2022

Penulis



DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR ISTILAH

Anomaly Based

Intrusi deteksi pada IDS berdasarkan anomali

Artificial Intelligence (Kecerdasan Buatan)

Sistem komputer yang memiliki kecerdasan layaknya manusia.

Artficial Neural Network

Sebuah teknik atau pendekatan pengolahan informasi yang terinspirasi oleh cara kerja sistem saraf biologis, khususnya pada sel otak manusia dalam memproses informasi.

Blockchain

Sebuah teknologi yang digunakan sebagai sistem penyimpanan data digital yang terhubung melalui kriptografi.

Blocking

Cara melindungi dengan cara membendung atau menahan suatu tindakan.

CDN (Content Delivery Network)

Kumpulan dari server global yang terletak di beberapa data center dan tersebar di berbagai negara. Jaringan ini berfungsi untuk mengirimkan konten dari server ke suatu website.

Centralize Log Management

Jenis solusi logging yang dirancang untuk mengumpulkan log dari beberapa server dan mengkonsolidasikan data.

CIA (Confidentiallity Integrity Availability)

Salah saru aturan dasar dalam menentukan keamanan suatu jaringan atau informasi.

Cloud Computing

Proses pengolahan sistem daya komputasi, melalui jaringan internet yang menghubungkan antara satu perangkat komputer dengan komputer lain, dalam waktu yang sama.

DDoS (Distributed Denial of Services)

Jenis serangan yang dilakukan dengan cara membanjiri lalu linras jaringan internet pada server, sistem, atau jaringan.

Dump

Proses mengeluarkand data dari database

Endpoint

Ujung jalur komunikasi dalam suatu jaringan.

Ensemble Classifier

Metode yang menggabungkan beberapa classifier agar dapat meningkatkan akurasi yang dihasilkan.

Float

Tipe data untuk objek numerik berupa bilangan desimal, baik positif atau negatif,

Host Based

Intrusi deteksi pada IDS berdasarkan host

IDS (Intrusion Detection System)

Sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan pada sebuah sistem atau jaringan.

Int (Integer)

Tipe data untuk objek numerik berupa bilangan bulat positif dan negative

Internet of Things

Suatu konsep atau program dimana sebuah objek memiliki kemampuan untuk mentransmisikan atau mengirimkan data melalui jaringan tanpa menggunakan bantuan perangkat komputer dan manusia.

Machine Learning (Pembelajaran Mesin)

Metode dalam sistem kecerdasan buatan yang mampu memodelkan data yang dimasukkan untuk kebutuhan atau memprediksi di masa mendatang.

Network Based

Intrusi deteksi pada IDS berdasarkan jaringan

Security Engineer

Orang yang bertugas memastikan data perusahaan yang tersimpan di dalam server tetap aman.

Signature Based

Intrusi deteksi pada IDS berdasarkan signature

System Administrator

Orang yang bertugas dan bertanggung jawan dalam pemeliharaan jaringan komputer perusahaan.

Threat Actor

orang atau sekumpulan orang/grup yang berpartisipasi dalam tindakan kejahatan siber.

INTISARI

Banyaknya serangan yang terjadi pada sebuah sistem elektronik dapat mengganggu kinerja sebuah industri atau bisnis. Salah satu serangan yang populer adalah serangan pada sisi jaringan dengan menguras habis bandwith atau resources yang dimiliki dengan kata lain serangan DDoS (*Distributed Denial of Service).* DDoS disebut sebagai senjata andalan para hacker karena telah terbukti menjadi ancaman permanen bagi pengguna, organisasi dan infrastruktur di internet.

Salah satu upaya untuk melakukan pendeteksian dan klasifikasi serangan DDoS adalah menggunakan *Machine Learning. Machine Learning* merupakan sebagai metode dalam sistem kecerdasan buatan yang mampu memodelkan data yang dimasukkan untuk kebutuhan atau memprediksi di masa mendatang. Penelitian ini bertujuan untuk menemukan model *Machine Learning* yang efektif digunakan dalam mendeteksi dan mengklasifikasikan serangan DDoS.

Penelitian ini menggunakan 4 model algoritma utama yaitu K-Nearest Neighbor, Naïve Bayes, Stochastic Gradient Descent, dan (XGBoost) eXtreme Gradient Boost. Dari keseluruhan model yang digunakan didapatilah kesimpulan bahwa eXtreme Gradient Boost (XGBoost) menunjukkan nilai akurasi tertinggi yaitu sebesar 89.4456%

Kata kunci: DDoS, Machine Learning, Serangan, Deteksi, Model

ABSTRACT

The number of attacks that occur on an electronic system can disrupt the performance of an industry or business. One of the popular attacks is an attack on the network side by draining bandwidth or called by DDoS (Distributed Denial of Service) attack. DDoS is referred to as the main weapon of hackers because it has proven to be a permanent threat to users, organizations and infrastructure on the internet.

One of the efforts to detect and classification DDoS attacks is using Machine Learning. Machine Learning as a method in an artificial intelligence system that is able to model the data entered for needs or predict the future. This study aims to find an effective Machine Learning model used in detecting and classification DDoS attacks.

This study uses 4 main models, K-Nearest Neighbor, Naïve Bayes, Stochastic Gradient Descent, and (XGBoost) eXtreme Gradient Boost. Of all the models used, eXtreme Gradient Boost produces the highest accuracy of 89.4456%

Keyword: *DDoS, Machine Learning, Attack, Detection, Model*