

**RANCANG BANGUN SISTEM PROXY MITIGASI DDOS
BERBASIS MACHINE LEARNING DAN BLOCKCHAIN**



UMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA

TUGAS AKHIR

Matthew Brandon Dani

0000036391

**PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG**

2023

RANCANG BANGUN SISTEM PROXY MITIGASI DDOS BERBASIS MACHINE LEARNING DAN BLOCKCHAIN



TUGAS AKHIR

Diajukan sebagai Salah Satu Syarat untuk Memperoleh
Gelar Sarjana Teknik Komputer

Matthew Brandon Dani

0000036391

**PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA**

TANGERANG

2023

i

Rancang Bangun Sistem Proxy Mitigasi DDoS berbasis Machine Learning dan Blockchain,
Matthew Brandon Dani, Universitas Multimedia Nusantara

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama : Matthew Brandon Dani

Nomor Induk Mahasiswa : 00000036391

Program studi : Teknik Komputer

Tugas akhir dengan judul:

RANCANG BANGUN SISTEM PROXY MITIGASI DDOS BERBASIS MACHINE LEARNING DAN BLOCKCHAIN

merupakan hasil karya saya sendiri bukan plagiat dari karya ilmiah yang ditulis oleh orang lain, dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk Tugas Akhir yang telah saya tempuh.

Tangerang, 16 Juni 2023


Brandon

(Matthew Brandon Dani)

UNIVERSITAS
MULTIMEDIA
NUSANTARA

HALAMAN PERSETUJUAN

Tugas akhir dengan judul

RANCANG BANGUN SISTEM PROXY MITIGASI DDOS BERBASIS MACHINE LEARNING DAN BLOCKCHAIN

Oleh

Nama : Matthew Brandon Dani
NIM : 00000036391
Program Studi : Teknik Komputer
Fakultas : Fakultas Teknik dan Informatika

Telah disetujui untuk diajukan pada

Sidang Ujian Tugas Akhir Universitas Multimedia Nusantara

Tangerang, 16 Juni 2023

Pembimbing



Samuel Hutagalung, M.T.I.
304038902

Pembimbing



Daren Kustuma Halim, S.Kom., M.Eng.Sc.
317129202

Ketua Teknik Komputer



Samuel Hutagalung, M.T.I.

HALAMAN PENGESAHAN

Tugas akhir dengan judul

RANCANG BANGUN SISTEM PROXY MITIGASI DDOS BERBASIS MACHINE LEARNING DAN BLOCKCHAIN

Oleh

Nama : Matthew Brandon Dani

NIM : 00000036391

Program Studi : Teknik Komputer

Fakultas : Fakultas Teknik dan Informatika

Telah diujikan pada hari Selasa, 27 Juni 2023

Pukul 15.00 s.d 17.00 dan dinyatakan

LULUS

Dengan susunan penguji sebagai berikut.

Ketua Sidang



Nabila Husna Shabrina, S.T., M. T.
321099301

Penguji



Monica Pratiwi, S.ST., M.T.
325059601

Pembimbing



Samuel Hutagalung, M.T.I.
304038902

Pembimbing



Daren Kusuma Halim, S.Kom., M.Eng.Sc
317129202

Ketua Teknik Komputer



Samuel Hutagalung, M.T.I.

iv

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas academica Universitas Multimedia Nusantara, saya yang bertanda tangan di bawah ini:

Nama : Matthew Brandon Dani
NIM : 00000036391
Program Studi : Teknik Komputer
Fakultas : Fakultas Teknik dan Informatika
Jenis Karya : *~~Tesis/Skripsi~~ **Tugas Akhir** (*coret salah satu)

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Multimedia Nusantara Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul.

RANCANG BANGUN SISTEM PROXY MITIGASI DDOS BERBASIS MACHINE LEARNING DAN BLOCKCHAIN

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini, Universitas Multimedia Nusantara berhak menyimpan, mengalihmediakan/mengalihformatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Tangerang, 16 Juni 2023

Yang menyatakan,



(Matthew Brandon Dani)

KATA PENGANTAR

Puji dan syukur kepada Tuhan Yang Maha Esa atas berkat yang diberikan kepada penulis selama proses pengerjaan dan pembuatan tugas akhir sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul “RANCANG BANGUN SISTEM PROXY MITIGASI DDOS BERBASIS MACHINE LEARNING DAN BLOCKCHAIN”. Dengan selesainya laporan tugas akhir ini, penulis mengucapkan syukur atas kelulusan penulis atas pendidikan strata satu program studi Teknik Komputer pada Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.

Tugas Akhir ini tidak dapat terselesaikan tanpa adanya dukungan dari berbagai pihak yang telah mendukung dan membimbing penulis. Oleh karena itu penulis ingin mengucapkan terima kasih kepada :

1. Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara.
2. Dr. Eng. Niki Prastomo, selaku Dekan Fakultas Universitas Multimedia Nusantara.
3. Samuel Hutagalung, M.T.I., selaku Ketua Program Studi Universitas Multimedia Nusantara dan juga sebagai Pembimbing pertama yang telah memberikan bimbingan, arahan, dan motivasi atas terselesainya tugas akhir ini.
4. Daren Kusuma Halim, S.Kom., M.Eng.Sc., sebagai Pembimbing kedua yang telah memberikan bimbingan, arahan, dan motivasi atas terselesainya tugas akhir ini.
5. Keluarga saya yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan tugas akhir ini.
6. Teman-teman Progam Studi Teknik Komputer Universitas Multimedia Nusantara angkatan 2019, yang telah bersama sama belajar dan berjuang untuk menyelesaikan pendidikan strata satu program studi teknik komputer.

7. Dan pihak-pihak lainnya yang tidak dapat disebutkan satu persatu yang telah membantu dalam pembuatan tugas akhir

Akhir kata, semoga karya ilmiah ini dapat bermanfaat dan menginspirasi bagi para pembaca sehingga dapat menjadi acuan dan dilanjutkan ke dalam penelitian terkait selanjutnya.

Tangerang, 16 Juni 2023

Brandon

(Matthew Brandon Dani)

UMMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA

RANCANG BANGUN SISTEM PROXY MITIGASI DDoS BERBASIS MACHINE LEARNING DAN BLOCKCHAIN

(Matthew Brandon Dani)

ABSTRAK

DDoS merupakan serangan pada jaringan komputer yang umum ditemukan. Namun sampai sekarang, masih belum ada solusi *intrusion prevention system* (IPS) yang *open-source* dan dapat memitigasinya secara efektif, keseluruhan, dan akurat. Hal ini juga didukung dengan terus meningkatnya angka serangan DDoS dari berbagai survei sumber referensi. Ketidakefektifannya karena DDoS memiliki metode dan teknik yang berbeda-beda sehingga akan menghasilkan serangan berupa pola stokastik. Pola stokastik akan sulit untuk dideteksi menggunakan metode "*threshold*" pada solusi IPS konvensional. Meningkatnya tren arsitektur sistem terdistribusi menggunakan jaringan internet juga akan memperbesar celah sistem untuk terserang jika tidak dirancang secara matang. Oleh karena itu dirancang dan dibangunlah sistem proxy terdistribusi yang dapat mendeteksi dan mengidentifikasi serangan DDoS menggunakan *machine learning* dan *blockchain*. Dilakukan penelitian menggunakan 2 metode *machine learning* yaitu pendekatan secara individual dan *timeseries*. Penelitian memakai beberapa algoritma *machine learning* seperti *Bidirectional LSTM*, SVM, Linear Regresion, dan lain-lain. Akan dibuat setiap model *machine learning* untuk setiap protokol jaringan komputer dan dianalisis menggunakan beberapa matriks pengujian. Untuk mendistribusikan informasi penyerang, digunakan *database* terdistribusi berbasis *blockchain* BigchainDB dan sistem konsensus. Penelitian menghasilkan model *machine learning* mendapatkan akurasi rata-rata di atas 95% dengan waktu deteksi kurang dari 1 detik dengan menggunakan *feature* dan data *pre-processing* yang dipilih. Walaupun terjadi *overfitting* akibat penggunaan dataset yang kecil, sehingga hanya dapat menjadi referensi penggunaan *machine learning* saja. Waktu distribusi data membutuhkan waktu 0,67 detik untuk tersebar ke setiap proxy terdistribusi. Sistem yang dirancang berhasil menunjukkan tingkat efektivitas yang lebih tinggi daripada IPS / IDS Snort yang *open-source* dan banyak dipakai sekarang, terutama pada tingkat deteksi *false positive*. Salah satunya adalah sistem ini dapat memitigasi serangan DDoS yang menggunakan IP *Spoofing* dengan tetap meneruskan paket yang normal.

Kata kunci: DDoS, Proxy, Sistem Terdistribusi, *Machine Learning*, *Blockchain*

RANCANG BANGUN SISTEM PROXY MITIGASI DDoS BERBASIS MACHINE LEARNING DAN BLOCKCHAIN

(Matthew Brandon Dani)

ABSTRACT (*English*)

DDoS is attack on computer network that is commonly found. But until now, there is still no intrusion prevention system (IPS) solutions that is open-source and can mitigate it effectively, comprehensively, and accurately. This is also supported by the continued increase in the number of DDoS attacks from various surveys of reference sources. The ineffectiveness is because DDoS has different methods and techniques that will result in the form of a stochastic pattern. Stochastic patterns will be difficult to detect using the "threshold" method on conventional IPS solutions. The increasing trend of distributed system architectures using internet networks will also increase the possibility of the system to be attacked if not designed carefully. Therefore a distributed proxy system was designed and built that can detect and identify DDoS attacks using machine learning and blockchain. Research was carried out using 2 machine learning methods the individual approach and the time series approach. Research uses several machine learning algorithms such as Bidirectional LSTM, SVM, Linear Regression, and others. Each machine learning model will be created for each computer network protocol and analyzed using several test matrices. To distribute attacker information, a distributed database based on blockchain BigchainDB and a consensus algorithm is used. Research shows that machine learning models obtaining an average accuracy of above 95% with a detection time of less than 1 second using selected features and pre-processing data. Even though there is overfitting due to the use of a small dataset, it can only be used as a reference for using machine learning. Data distribution time takes 0.67 seconds to spread to each distributed proxy. The successfully designed system shows a higher level of effectiveness than the open-source and widely used IPS / IDS Snort, especially at the false positive detection rate. One of them is that this system can mitigate DDoS attacks using IP Spoofing while still forwarding normal packets.

Keywords: *DDoS, Proxy, Distributed System, Machine Learning, Blockchain*

DAFTAR ISI

HALAMAN PERNYATAAN TIDAK PLAGIAT.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS.....	v
KATA PENGANTAR.....	vi
ABSTRAK.....	viii
<i>ABSTRACT (English)</i>	ix
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
DAFTAR LAMPIRAN.....	xix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah.....	7
1.3 Batasan Penelitian.....	7
1.4 Tujuan Penelitian.....	8
1.5 Manfaat Penelitian.....	8
1.6 Sistematika Penulisan.....	9
BAB II TINJAUAN PUSTAKA.....	11
2.1 Penelitian Terdahulu.....	11
2.2 Tinjauan Teori.....	35
2.2.1 OSI Layer.....	35
2.2.1.1 TCP.....	36
2.2.1.2 UDP.....	38
2.2.1.3 ICMP.....	39
2.2.1.4 HTTP.....	39
2.2.2 IP Tables.....	40
2.2.3 <i>Intrusion Prevention System dan Intrusion Detection System</i>	40
2.2.3.1 Snort.....	42
2.2.4 NetfilterQueue.....	43

2.2.5	Reverse Proxy	43
2.2.5.1	Concurent Connection	44
2.2.6	Python Socket	44
2.2.7	Python Multithreading	45
2.2.8	BigchainDB	46
2.2.9	Democracy JS	47
2.2.10	Standar Deviasi dan Variansi	48
2.2.11	Machine Learning	48
2.2.12	Bidirectional LSTM	50
2.2.13	Imbalance dataset	51
2.2.13.1	Smote	52
2.2.14	ReactJS	52
2.2.15	Express JS	53
2.2.16	Hping3	53
2.2.17	Jmeter	54
2.2.18	IP Spoofing	54
2.3	Simpulan	54
BAB III ANALISIS DAN PERANCANGAN SISTEM		57
3.1	Metode Penelitian	57
3.2	Studi literatur	57
3.3	Arsitektur General Sistem Proxy Mitigasi DDoS berbasis Machine Learning dan Blockchain	58
3.4	Alur Sistem Proxy Mitigasi DDoS berbasis Machine Learning dan Blockchain	59
3.5	Analisis Features yang akan Dipakai	62
3.6	Perancangan Sistem Proxy	72
3.7	Pengambilan Dataset	75
3.8	Perancangan Machine Learning	77
3.9	Perancangan Sistem Firewall	85
3.10	Perancangan Sistem Distribusi Data	87
3.10.1	Perancangan database terdistribusi BigchainDB	87
3.10.2	Perancangan Sistem Backend	88

3.10.3	Perancangan Sistem Frontend.....	90
3.10.4	Analisa Kecepatan Persebaran Data	91
3.11	Perancangan Deployment Infratraktur Sistem.....	93
3.12	Perbandingan dengan IDS / IPS Snort.....	93
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM		95
4.1	Spesifikasi Sistem dan Testbed	95
4.2	Implementasi Sistem	97
4.2.1	Pembangunan Sistem Proxy	98
4.2.2	Pembangunan Machine Learning	103
4.2.3	Pembangunan Sistem Firewall	109
4.2.4	Pembangunan Sistem Distribusi Data	111
4.2.5	Pembangunan IPS / IDS Snort	121
4.3	Hasil dan analisis Pengujian Sistem	124
4.3.1	Analisis Hasil Evaluasi Performa Machine Learning	124
4.3.2	Analisis Hasil Evaluasi Sistem Reverse Proxy	140
4.3.3	Analisis Hasil Evaluasi Sistem Distribusi Data.....	143
4.3.4	Analisis Hasil Perbandingan dengan IDS / IPS Snort.....	146
4.4	Kendala dan Solusi penelitian	148
BAB V SIMPULAN DAN SARAN.....		149
5.1	Simpulan.....	149
5.2	Saran.....	151
DAFTAR PUSTAKA.....		153
LAMPIRAN.....		157

DAFTAR TABEL

Tabel 2.1 Features yang Digunakan dalam Deteksi Serangan DDoS menggunakan SVM.....	16
Tabel 2.2 Tabel Snort Rule Syntax.....	42
Tabel 2.3 Operasi Data BigchainDB	46
Tabel 3.1 Ilustrasi Normalisasi Dataset	79
Tabel 3.2 List API Endpoint Backend	89
Tabel 4.1 Hasil Dataset yang Terkumpul	104
Tabel 4.2 Perbandingan Dataset Sebelum dan Sesudah Balancing	105
Tabel 4.3 Perbandingan Dataset Normalisasi	108
Tabel 4.4 Perbandingan Hasil Performa Machine Learning dengan Classification Report.....	128
Tabel 4.5 Perbandingan Hasil Performa Machine Learning dengan Time Prediction	134
Tabel 4.6 Perbandingan Hasil Performa Machine Learning Identifikasi dengan Classification Matrix	135
Tabel 4.7 Perbandingan Hasil Performa Machine Learning Identifikasi dengan Waktu Prediksi	137
Tabel 4.8 Perbandingan Hasil Performa Machine Learning dengan Metode yang Berbeda	139
Tabel 4.9 Perbandingan Rata Rata Penggunaan CPU antara Sistem yang Dibuat dengan Aplikasi Snort.....	147
Tabel 4.10 Perbandingan Waktu TTM Sistem yang Dibuat dengan Aplikasi Snort	147

DAFTAR GAMBAR

Gambar 1.1	Gambaran Umum Serangan DDoS.....	2
Gambar 1.2	Grafik Trend Global Serangan DDoS	3
Gambar 1.3	Ilustrasi Perbedaan Sistem Distributed, Centralized, dan Decentralized	5
Gambar 1.4	Ilustrasi Proxy Terdistribusi	6
Gambar 2.1	Ilustrasi serangan TCP SYN	12
Gambar 2.2	Proses Deteksi Serangan DDoS secara individual	14
Gambar 2.3	Ilustrasi Klasifikasi Algoritma Machine Learning SVM.....	16
Gambar 2.4	Proses Deteksi menggunakan LSTM.....	19
Gambar 2.5	Proses Transformasi Dataset LSTM.....	20
Gambar 2.6	Korelasi antara time window dengan akurasi model machine learning LSTM	21
Gambar 2.7	Arsitektur Pembagian Informasi Penyerang menggunakan Blockchain dan IPFS	23
Gambar 2.8	Sequence Diagram Pembagian Informasi Identitas Penyerang menggunakan Blockchain dan IPFS	24
Gambar 2.9	Perbandingan input 1000 data dengan BigchainDB dan Amazon QLDB	26
Gambar 2.10	Perbandingan membaca 1000 data dengan BigchainDB dan Amazon QLDB	26
Gambar 2.11	Karakteristik Serangan DDOS.....	30
Gambar 2.12	Hasil Pengujian dan Analisis penggunaan features MEFF	30
Gambar 2.13	Hasil Pengujian dan Analisis Penggunaan Multicore dan Multithread pada Proxy Server	32
Gambar 2.14	Ilustrasi Ketergantungan OSI Layer	35
Gambar 2.15	Alur handshaking TCP	36
Gambar 2.16	TCP Segmen	37
Gambar 2.17	UDP Segmen.....	38

Gambar 2.18 ICMP Segmen	39
Gambar 2.19 Implementasi IDS dan IPS.....	41
Gambar 2.20 Implementasi Reverse Proxy	43
Gambar 2.21 Contoh Implementasi Socket untuk Reverse Proxy	45
Gambar 2.22 Contoh Implementasi Multithreading Socket untuk Reverse Proxy.....	45
Gambar 2.23 Penggunaan DemocracyJS.....	47
Gambar 2.24 Struktur LSTM.....	50
Gambar 2.25 Struktur Bidirectional LSTM.....	51
Gambar 2.26 Ilustrasi Teknik SMOTE untuk menangani masalah dataset tidak seimbang.....	52
Gambar 2.27 Diagram State of The Art	56
Gambar 3.1 Diagram tahapan penelitian	57
Gambar 3.2 Diagram Arsitektur Sistem secara General	58
Gambar 3.3 Sequence Diagram untuk Deteksi Paket.....	59
Gambar 3.4 Sequence Diagram untuk Persebaran Data Informasi Penyerang	60
Gambar 3.5 Sequence Diagram untuk Admin Membuat Akun dan Melakukan Operasi Database	61
Gambar 3.6 Alur Kerja Sistem Proxy Mitigasi DDoS berbasis Machine Learning dan DDoS	62
Gambar 3.7 Alur Analisis Features yang akan Dipakai.....	63
Gambar 3.8 Potongan Kode Program Random Request UDP	64
Gambar 3.9 Potongan Kode Program Video Streaming UDP.....	65
Gambar 3.10 Potongan Kode Bash Script ICMP Normal	65
Gambar 3.11 Potongan Kode Program HTTP GET Flood	66
Gambar 3.12 Potongan Kode Program HTTP GET Flood 2	66
Gambar 3.13 Potongan Kode Program HTTP GET Flood 3	66
Gambar 3.14 Potongan Kode Firewall Sniffer	67
Gambar 3.15 Contoh Observasi Menggunakan Software Wireshark	69

Gambar 3.16 Kode SVM features Importance	69
Gambar 3.17 Hasil Plot SVM features Importance.....	70
Gambar 3.18 Alur Kerja Analisis features importance SVM.....	70
Gambar 3.19 Arsitektur Sistem Reverse Proxy	72
Gambar 3.20 Arsitektur Multithreading Socket.....	73
Gambar 3.21 Sequence diagram untuk proses pengambilan dataset individual	74
Gambar 3.22 Perbedaan Metode Individual dan Timeseries	74
Gambar 3.23 Arsitektur Pengambilan Dataset	76
Gambar 3.24 Cara Kerja Dataset Individu	76
Gambar 3.25 Cara Kerja Dataset Timeseries	77
Gambar 3.26 Potongan Kode SMOTE untuk Balancing Dataset	78
Gambar 3.27 Ilustrasi Proses Balancing SMOTE	78
Gambar 3.28 Arsitektur Machine Learning DNN	81
Gambar 3.29 Arsitektur Machine Learning LSTM	82
Gambar 3.30 Perbedaan Atomic dan Composite.....	83
Gambar 3.31 Ilustrasi Metode Karakteristik Paket Terbanyak	84
Gambar 3.32 Arsitektur Sistem Firewall dan Proxy	86
Gambar 3.33 Diagram 2 Fase Machine Learning.....	86
Gambar 3.34 Database Schema	88
Gambar 3.35 Rancangan Frontend	91
Gambar 3.36 Alur Evaluasi Sistem Distribusi Data	92
Gambar 3.37 Ilustrasi Deployment Sistem Proxy Mitigasi DDoS.....	93
Gambar 4.1 VMware Synchronize time.....	95
Gambar 4.2 Potongan Kode Webserver	96
Gambar 4.3 Arsitektur Reverse Proxy.....	97
Gambar 4.4 Arsitektur Modul Proxy.....	98
Gambar 4.5 Potongan Pembuatan Thread TCP.....	99
Gambar 4.6 Potongan Kode dan Contoh File Konfigurasi Proxy Server	99
Gambar 4.7 Potongan Kode Thread Safe Logging.....	100

Gambar 4.8 Potongan Kode Data Parser	100
Gambar 4.9 Tampilan Proxy Server	101
Gambar 4.10 Arsitektur Firewall Server	101
Gambar 4.11 Potongan Kode fungsi Filter Firewall.....	102
Gambar 4.12 Alur Kerja Pembangunan Model Machine Learning	102
Gambar 4.13 Potongan Kode Perubah String menjadi Numerik Bytes	103
Gambar 4.14 Ilustrasi Proses Transformasi Dataset LSTM	104
Gambar 4.15 Potongan Kode Transformasi Dataset menjadi 3 Dimensional Matriks	104
Gambar 4.16 Potongan Kode Teknik SMOTE dan Perbedaan Jumlah Dataset.....	105
Gambar 4.17 Potongan Kode Proses Normalisasi Dataset	106
Gambar 4.18 Potongan Kode Eksport Instance.....	106
Gambar 4.19 Potongan Kode Pembagian Dataset Training dan Testing....	106
Gambar 4.20 Potongan Kode Pembuatan Model Machine Learning.....	107
Gambar 4.21 Potongan Kode Training Machine Learning	107
Gambar 4.22 Arsitektur Sistem Firewall.....	107
Gambar 4.23 Potongan Kode Implementasi Machine Learning pada Firewall Controller.....	108
Gambar 4.24 Potongan Kode Objek Signature.....	108
Gambar 4.25 Potongan Kode Implementasi Firewall	108
Gambar 4.26 Tampilan Program Firewall saat Bekerja.....	109
Gambar 4.27 Arsitektur Sistem Distribusi Data.....	109
Gambar 4.28 Alur Instalasi BigchainDB Network	110
Gambar 4.29 Ilustrasi Infrastruktur BigchainDB Network	110
Gambar 4.30 Tampilan Tendermint Init.....	111
Gambar 4.31 Data public key node dan Node Id	111
Gambar 4.32 Isi File genesis.json Tendermint	112
Gambar 4.33 Konfigurasi Tendermint Config.toml.....	113
Gambar 4.34 Konfigurasi BigchainDB	114

Gambar 4.35 Konfigurasi Firewall untuk Tendermint.....	114
Gambar 4.36 Tampilan BigchainDB setelah Berjalan	114
Gambar 4.37 Struktur Folder Backend.....	115
Gambar 4.38 Arsitektur Modul Backend.....	115
Gambar 4.39 Potongan Kode Database untuk Operasi Data	116
Gambar 4.40 Potongan Kode Konfigurasi DemocracyJS.....	116
Gambar 4.41 Potongan Kode Pub/Sub democracyJS	117
Gambar 4.42 Potongan Kode Backend CronJob	117
Gambar 4.43 Tampilan Sistem Backend	118
Gambar 4.44 Arsitektur Sistem Backend	118
Gambar 4.45 Tampilan Sistem Frontend	119
Gambar 4.46 Instalasi Snort	120
Gambar 4.47 Prompt Instalasi Snort	120
Gambar 4.48 Aplikasi Snort.....	120
Gambar 4.49 Isi dari snort.conf pada Aplikasi Snort	121
Gambar 4.50 Custom Ruleset Aplikasi Snort	121
Gambar 4.51 Tampilan Ketika Program Snort Dijalankan	122
Gambar 4.52 Tampilan Pengambilan Data Rata Rata Penggunaan CPU ..	129
Gambar 4.53 Hasil Penelitian Uji Proxy 1.....	129
Gambar 4.54 Hasil Penelitian Uji Proxy 2.....	130
Gambar 4.55 Hasil Penelitian Uji Proxy 3.....	130
Gambar 4.56 Hasil Penelitian Uji Proxy 4.....	131
Gambar 4.57 Hasil Penelitian Uji Proxy 5.....	131
Gambar 4.58 Hasil Penelitian Uji Proxy 6.....	132
Gambar 4.59 Hasil Penelitian Uji Sistem Distribusi 1.....	133
Gambar 4.60 Hasil Penelitian Uji Sistem Distribusi 2.....	133
Gambar 4.61 Hasil Penelitian Uji Sistem Distribusi 3.....	134

DAFTAR LAMPIRAN

Lampiran A. Hasil Turnitin.....	156
Lampiran B. Form Konsultasi Skripsi Pembimbing 1.....	159
Lampiran C. Form Konsultasi Skripsi Pembimbing 2.....	160



UMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA