SKRIPSI

PENGEMBANGAN WEB APPLICATION FIREWALL BERBASIS MACHINE LEARNING MENGGUNAKAN PSO-SVM DENGAN PENDEKATAN HYBRID: SIGNATURE DAN ANOMALY BASED

NOVANDI KEVIN PRATAMA
NPM 20081010005

DOSEN PEMBIMBING
Achmad Junaidi, S.Kom., M.Kom.
Afina Lina Nurlaili, S.Kom., M.Kom.

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA
SURABAYA
2024

`

SKRIPSI

PENGEMBANGAN WEB APPLICATION FIREWALL BERBASIS MACHINE LEARNING MENGGUNAKAN PSO-SVM DENGAN PENDEKATAN HYBRID: SIGNATURE DAN ANOMALY BASED

NOVANDI KEVIN PRATAMA
NPM 20081010005

DOSEN PEMBIMBING
Achmad Junaidi, S.Kom., M.Kom.
Afina Lina Nurlaili, S.Kom., M.Kom.

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA
SURABAYA

2024

`

Halaman ini sengaja dikosongkan

LEMBAR PENGESAHAN

PENGEMBANGAN WEB APPLICATION FIREWALL BERBASIS MACHINE LEARNING MENGGUNAKAN PSO-SVM DENGAN PENDEKATAN HYBRID: SIGNATURE DAN ANOMALY BASED

Oleh :

NOVANDI KEVIN PRATAMA

NPM. 20081010005

Telah dipertahankan di hadapan dan diterima oleh Tim Penguji Skripsi Prodi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jawa Timur Pada tanggal 30 Agustus 2024

Achmad Junaidi, S.Kom., M.Kom.
NPT. 3 7811 04 0199 1 ..... **(Pembimbing I)**

Afina Lina Nurlaili, S.Kom., M.Kom.
NIP. 1993121 3202203 2010 ..... **(Pembimbing II)**

Dr. Eng. Ir. Anggraini Puspita Sari, ST., MT.
NPT. 222198 60 816400 ..... **(Ketua Penguji)**

Agung Mustika Rizki, S.Kom., M.Kom.
NIP. 19930725 202203 1008 ..... **(Anggota Penguji)**

Mengetahui,
Dekan Fakultas Ilmu Komputer

Prof. Dr. Ir. Novirina Hendrasarie, MT
NIP. 19681126 199403 2 001

`

Halaman ini sengaja dikosongkan

LEMBAR PERSETUJUAN

PENGEMBANGAN WEB APPLICATION FIREWALL BERBASIS MACHINE LEARNING MENGGUNAKAN PSO-SVM DENGAN PENDEKATAN HYBRID: SIGNATURE DAN ANOMALY BASED

Oleh :

NOVANDI KEVIN PRATAMA

NPM. 20081010005

Menyetujui,

Koordinator Program Studi Informatika

Fakultas Ilmu Komputer

Fetty Tri Anggraeny, S.Kom., M.Kom.

NIP. 19820211 2021212 005

SURAT PERNYATAAN ORISINALITAS

Yang bertandatangan di bawah ini:

Nama Mahasiswa	:	NOVANDI KEVIN PRATAMA
Program Studi	:	Informatika
Dosen Pembimbing	:	1. Achmad Junaidi, S.Kom., M.Kom.
		2. Afina Lina Nurlaili, S.Kom., M.Kom.

dengan ini menyatakan bahwa isi sebagian maupun keseluruhan skripsi dengan judul:

PENGEMBANGAN WEB APPLICATION FIREWALL BERBASIS MACHINE LEARNING MENGGUNAKAN PSO-SVM DENGAN PENDEKATAN HYBRID: SIGNATURE DAN ANOMALY BASED

adalah benar-benar hasil karya intelektual mandiri, diselesaikan tanpa menggunakan bahan-bahan yang tidak diizinkan dan bukan merupakan karya pihak lain yang saya akui sebagai karya sendiri. Semua referensi yang dikutip maupun dirujuk telah ditulis secara lengkap pada daftar pustaka. Apabila ternyata pernyataan ini tidak benar, saya bersedia menerima sanksi sesuai peraturan yang berlaku.

Surabaya, 4 OKTOBER 2024

Yang Membuat Pernyataan,

NOVANDI KEVIN PRATAMA

NPM. 20081010005

`

Halaman ini sengaja dikosongkan

`

ABSTRAK

Nama Mahasiswa / NPM	:	Novandi Kevin Pratama / 20081010005
Judul Skripsi	:	Pengembangan Web Application Firewall Berbasis *Machine Learning* Menggunakan PSO-SVM Dengan Pendekatan *Hybrid*: *Signature* Dan *Anomaly Based*
Dosen Pembimbing	:	1. Achmad Junaidi, S.Kom., M.Kom. 2. Afina Lina Nurlaili, S.Kom., M.Kom.

Penggunaan aplikasi web merupakan hal yang esensial dalam pendidikan dan bisnis, memfasilitasi akses pembelajaran daring dan komunikasi tim. Namun, keamanan aplikasi web menjadi krusial karena peningkatan jumlah pengguna dan data sensitif yang disimpan. Serangan seperti *SQL Injection* mengancam aplikasi web yang tidak memvalidasi input pengguna dengan benar. Web Application Firewall (WAF) melindungi aplikasi web dengan pendekatan berbasis *signature* dan *anomaly*. *Signature based* mendeteksi serangan berdasarkan pola yang dikenal, tetapi tidak efektif untuk serangan baru. Anomaly based mendeteksi pola mencurigakan menggunakan *machine learning* namun lambat untuk deteksi real-time. Pendekatan hybrid menggabungkan kedua metode tersebut untuk menutupi kelemahan masing-masing. Penelitian ini menerapkan PSO-SVM untuk meningkatkan deteksi serangan pada permintaan HTTP. Kombinasi pendekatan berbasis *signature* dan *anomaly*, dioptimalkan menggunakan PSO, bertujuan meningkatkan deteksi serangan baru dan mengurangi jumlah serangan yang lolos. Evaluasi dilakukan dengan berbagai skenario pengujian, memanfaatkan *fitness function* untuk mengoptimalkan parameter SVM. Hasil akhir menunjukkan peningkatan signifikan dalam deteksi serangan dan kinerja sistem keamanan. Dari berbagai skenario pengujian mendapatkan model paling optimal dengan nilai rata-rata akurasi sebesar 97,80%. Namun, hasil evaluasi kecepatan dari model terbaik menunjukkan bahwa metode *anomaly-based* dengan PSO-SVM memiliki waktu deteksi yang lebih lambat dibandingkan *signature-based*, dengan perbedaan waktu deteksi tercepat masing-masing metode mencapai hingga 8,98 ms. Meski demikian, keunggulan *anomaly-based* dalam mendeteksi serangan baru tetap memberikan kontribusi penting dalam menjaga keamanan sistem.

Kata kunci : Web Application Firewall, *Particle Swarm Optimization*, *Support Vector Machine*, Deteksi Serangan, *signature based* dan *anomaly based*.

`

Halaman ini sengaja dikosongkan

`

ABSTRACT

Student Name / NPM	:	Novandi Kevin Pratama / 20081010005
Thesis Title	:	Development of a Machine Learning-Based Web Application Firewall Using PSO-SVM with a Hybrid Approach: Signature and Anomaly-Based
Advisor	:	1. Achmad Junaidi, S.Kom., M.Kom. 2. Afina Lina Nurlaili, S.Kom., M.Kom.

The use of web applications is essential in education and business, facilitating access to online learning and team communication. However, web application security becomes crucial due to the increasing number of users and the sensitive data stored. Attacks such as SQL Injection threaten web applications that do not properly validate user input. A Web Application Firewall (WAF) protects web applications using signature-based and anomaly-based approaches. Signature-based detection identifies attacks based on known patterns but is ineffective against new attacks. Anomaly-based detection identifies suspicious patterns using machine learning but is slow for real-time detection. A hybrid approach combines both methods to cover each other's weaknesses. This research implements PSO-SVM to improve attack detection on HTTP requests. The combination of signature-based and anomaly-based approaches, optimized using PSO, aims to enhance the detection of new attacks and reduce the number of successful attacks. Evaluation is conducted with various testing scenarios, utilizing a fitness function to optimize SVM parameters. The final results show a significant improvement in attack detection and security system performance. From various testing scenarios, the most optimal model achieved an average accuracy of 97.80%. However, the evaluation of the best model's speed shows that the anomaly-based method with PSO-SVM has a slower detection time compared to the signature-based method, with the fastest detection time difference between the methods reaching up to 8.98 ms. Nonetheless, the advantage of the anomaly-based method in detecting new attacks still provides a crucial contribution to maintaining system security.

Keywords : Web Application Firewall, Particle Swarm Optimization, Support Vector Machine, Threat Detection, Signature based and anomaly based.

`

Halaman ini sengaja dikosongkan

`

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala rahmat, hidayah dan karunia-Nya kepada penulis sehingga skripsi dengan judul **"Pengembangan *Web Application Firewall* Berbasis *Machine Learning* Menggunakan PSO-SVM Dengan Pendekatan Hybrid: *Signature* Dan *Anomaly Based*"** dapat terselesaikan dengan baik.

Penulis mengucapkan terima kasih kepada Bapak Achmad Junaidi, S.Kom., M.Kom. selaku Dosen Pembimbing utama yang telah meluangkan waktunya untuk memberikan bimbingan, nasehat serta motivasi kepada penulis. Dan penulis juga banyak menerima bantuan dari berbagai pihak, baik itu berupa moril, spiritual maupun materiil. Untuk itu penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Ir. Akhmad Fauzi, MMT. selaku Rektor Universitas Pembangunan Nasional "Veteran" Jawa Timur.
2. Ibu Prof. Dr. Ir. Novirina Hendrasarie, MT. selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jawa Timur.
3. Ibu Fetty Tri Anggraeny, S.Kom, M.Kom. selaku Koordinator Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jawa Timur yang telah membantu penulis dalam menjalani perkuliahan baik dari sisi akademis maupun non-akademis. .
4. Bapak Achmad Junaidi, S.Kom., M.Kom. selaku Dosen Pembimbing satu yang telah banyak membantu penulis dari awal perkuliahan, dukungan berupa koreksi, arahan, dan juga saran dalam proses penyelesaian skripsi ini hingga terselesaikannya skripsi ini.
5. Ibu Afina Lina Nurlaili, S.Kom., M.Kom. selaku Dosen Pembimbing dua yang telah membantu penulis dalam proses pengerjaan skripsi ini dengan sabar serta memberi dukungan berupa koreksi, arahan, dan juga saran dalam proses penyelesaian skripsi ini hingga terselesaikannya skripsi ini.
6. Ibu Dr. Eng. Ir. Anggraini Puspita Sari, ST., MT. Selaku Dosen Penguji 1 yang telah mengarahkan penulis dalam pengerjaan skripsi ini sehingga skripsi ini ditulis dengan baik.
7. Bapak Agung Mustika Rizki, S.Kom., M.Kom. Selaku Dosen Penguji 2 yang telah mengarahkan penulis dalam pengerjaan skripsi ini sehingga skripsi ini ditulis dengan baik

`

8. Seluruh Dosen Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur atas segala ilmu pengetahuan yang diberikan kepada penulis selama masa perkuliahan dan memberikan pengalaman berharga bagi penulis baik dari sisi akademis maupun non-akademis.
9. Seluruh keluarga saya, terutama ibu saya, yang telah merawat, menerima, dan memberikan apa pun yang penulis butuhkan sepanjang waktu tanpa menghiraukan lelahnya sejak penulis lahir sehingga penulis dapat menyelesaikan skripsi ini yang kebaikan mereka tidak mungkin penulis balas dengan sepadan hingga akhir hayat.
10. Rekan-rekan mahasiswa Informatika angkatan 2020 yang telah memberikan dukungan, semangat, serta kebersamaan selama masa perkuliahan yang sangat membantu penulis dalam menyelesaikan skripsi ini.

Penulis menyadari bahwa di dalam penyusunan skripsi ini banyak terdapat kekurangan. Untuk itu kritik dan saran yang membangun dari semua pihak sangat diharapkan demi kesempurnaan penulisan skripsi ini. Akhirnya, dengan segala keterbatasan yang penulis miliki semoga laporan ini dapat bermanfaat bagi semua pihak umumnya dan penulis pada khususnya.

Surabaya, 20 September 2024

Novandi Kevin Pratama

`

DAFTAR ISI

LEMBAR PENGESAHAN ..... **iii**
SURAT PERNYATAAN ORISINALITAS ..... **v**
ABSTRAK ..... **vii**
ABSTRACT ..... **ix**
KATA PENGANTAR ..... **xi**
DAFTAR ISI ..... **xiii**
DAFTAR TABEL ..... **xvii**
DAFTAR GAMBAR ..... **xix**
DAFTAR PSEUDOCODE ..... **xxi**
BAB I PENDAHULUAN **1**
1.1. Latar Belakang 1
1.2. Rumusan Masalah 3
1.3. Tujuan Penelitian 3
1.4. Manfaat Penelitian 3
1.5. Batasan Masalah 4
BAB II TINJAUAN PUSTAKA **5**
2.1. Penelitian Terdahulu 5
2.2. Landasan Teori 8
2.2.1. *Web Application Firewall* (WAF) 9
2.2.2. SQL Injection 9
2.2.3. *Cross-Site Scripting* (XSS) 10
2.2.4. Buffer Overflow 13
2.2.5. OS Command Injection 13
2.2.6. Path Traversal 14
2.2.7. Signature-based Detection 14
2.2.8. Anomaly-based Detection 15
2.2.9. *Particle Swarn Optimization* (PSO) 15
2.2.10. *Support Vector Machine* (SVM) 16
2.2.11. Min-Max Scalling 19
2.2.12. JSON (*JavaScript Object Notation*) 19
2.2.13. *Sequential Minimal Optimization* (SMO) 20

2.2.14. JSON *Parsing* 23
2.2.15. Confusion matrix 23
BAB III METODOLOGI PENELITIAN 27
3.1. Tahapan Penelitian 27
3.2. Pengumpulan Data 28
3.3. Pra-proses Data 31
3.4. Ekstraksi Fitur 32
3.5. Normalisasi Data 33
3.6. Perancangan WAF 34
3.6.1. Signature Based Detection 35
3.6.2. Anomaly-Based Detection 35
3.7. Skenario Pengujian 36
3.7.1. Skenario Pertama 36
3.7.2. Skenario Kedua 37
3.7.3. Skenario Ketiga 37
3.7.4. Skenario Keempat 37
3.7.5. Skenario Kelima 37
BAB IV HASIL DAN PEMBAHASAN 39
4.1. Penerapan Kode 39
4.1.1. Standarisasi Dataset ECML PKDD 2007 39
4.1.2. Standarisasi Dataset CSIC 2010 41
4.1.3. Ekstraksi Fitur 43
4.1.4. Penerapan *Min-Max Scaling* 53
4.1.5. SVM yang dioptimalkan oleh PSO 54
4.2. Hasil Skenario Pengujian 60
4.2.1. Skenario Pengujian Pertama 60
4.2.2. Skenario Pengujian Kedua 71
4.2.3. Skenario Pengujian Ketiga 78
4.2.4. Skenario Pengujian Keempat 86
4.2.5. Skenario Pengujian Kelima 93
4.3. Perbandingan Hasil Evaluasi 96
4.4. Perbandingan Kecepatan Deteksi Antar Pendekatan 98
BAB V PENUTUP 101

`

5.1. Kesimpulan 101
5.2. Saran.....102
DAFTAR PUSTAKA 103

`

Halaman ini sengaja dikosongkan

`

DAFTAR TABEL

Tabel 2. 1. Perbandingan Penelitian Terdahulu 5
Tabel 2. 2. *Confusion Matrix* 24
Tabel 3. 1. Sampel Contoh Dataset ECML PKDD 2007 dan CSIC 2010 28
Tabel 3. 2. Sebaran Data..... 30
Tabel 3. 3. Fitur yang digunakan..... 32
Tabel 4. 1. Sampel Kata Kunci Berbahaya 52
Tabel 4. 2. Evaluasi Dataset ECML pada Pengujian Rasio 85:15 61
Tabel 4. 3. Evaluasi Dataset CSIC pada Pengujian Rasio 85:15 63
Tabel 4. 4. Evaluasi Dataset ECML pada Pengujian Rasio 80:20 64
Tabel 4. 5. Evaluasi Dataset CSIC pada Pengujian Rasio 80:20 66
Tabel 4. 6. Evaluasi Dataset ECML pada Pengujian Rasio 75:25 67
Tabel 4. 7. Evaluasi Dataset CSIC pada Pengujian Rasio 75:25 69
Tabel 4. 8. Nilai Matriks Pengujian Rasio Pembagian Data 70
Tabel 4. 9. Evaluasi Dataset ECML pada Pengujian *w* 1 71
Tabel 4. 10. Evaluasi Dataset CSIC pada Pengujian *w* 1 73
Tabel 4. 11. Evaluasi Dataset ECML pada Pengujian w 1.5 74
Tabel 4. 12. Evaluasi Dataset CSIC pada Pengujian *w 1.5* 76
Tabel 4. 13. Nilai Matriks Pengujian Parameter *w* 78
Tabel 4. 14. Evaluasi Dataset ECML pada Pengujian *c1* 2 79
Tabel 4. 15. Evaluasi Dataset CSIC pada Pengujian *c1* 2 80
Tabel 4. 16. Evaluasi Dataset ECML pada Pengujian *c1* 3 82
Tabel 4. 17. Evaluasi Dataset CSIC pada Pengujian *c1* 3 84
Tabel 4. 18. Nilai Matriks Pengujian Parameter *c1* 85
Tabel 4. 19. Evaluasi Dataset ECML pada Pengujian *c2* 2 86
Tabel 4. 20. Evaluasi Dataset CSIC pada Pengujian *c2* 2 88
Tabel 4. 21. Evaluasi Dataset ECML pada Pengujian *c2* 3 89
Tabel 4. 22. Evaluasi Dataset CSIC pada Pengujian *c2* 3 91
Tabel 4. 23. Nilai Matriks Pengujian Parameter *c2* 92
Tabel 4. 24. Evaluasi Dataset ECML pada Pengujian Kelima 93
Tabel 4. 25. Evaluasi Dataset CSIC pada Pengujian Kelima 94

`

Tabel 4. 26. Perbandingan Hasil Evaluasi ECML Antar Model.....97
Tabel 4. 27. Perbandingan Hasil Evaluasi CSIC Antar Model.....98

`

DAFTAR GAMBAR

Gambar 2. 1. Skenario *SQL Injection Attack* 9
Gambar 2. 2. Pola *Reflected XSS* 10
Gambar 2. 3. *Pola Stored XSS* 11
Gambar 2. 4. Pola *DOM-based XSS*..... 12
Gambar 2. 5. *Hyperplane Support Vector Machine* (SVM) 17
Gambar 3. 1. Tahapan Penelitian 27
Gambar 3. 2. Sampel Data CSIC 2010..... 31
Gambar 3. 3. Hasil Konversi JSON 31
Gambar 3. 4. Contoh Perhitungan Fitur Panjang *Path* 33
Gambar 3. 5. Analisis Fitur Dataset CSIC 33
Gambar 3. 6. Alur Kerja WAF 34
Gambar 4. 1. Sampel Hasil *Parsing* JSON Dataset ECML PKDD 2007..... 41
Gambar 4. 2. Sampel Hasil *Parsing* JSON CSIC 2010 43
Gambar 4. 3. Hasil Sampel Keseluruhan Ekstraksi Fitur..... 53
Gambar 4. 4. Hasil Sampel Proses *Min-Max Scaling* 54
Gambar 4. 5. Hasil Evaluasi ECML Sesi Terbaik Rasio 85:15 62
Gambar 4. 6. *Confusion Matrix* Dataset ECML pada Pengujian Rasio 85:15.... 62
Gambar 4. 7. Hasil Evaluasi CSIC Sesi Terbaik Rasio 85:15 63
Gambar 4. 8. *Confusion Matrix* Dataset CSIC pada Pengujian Rasio 85:15..... 63
Gambar 4. 9. Hasil Evaluasi ECML Sesi Terbaik Rasio 80:20 65
Gambar 4. 10. *Confusion Matrix* Dataset ECML pada Pengujian Rasio 80:20.. 65
Gambar 4. 11. Hasil Evaluasi CSIC Sesi Terbaik Rasio 80:20..... 66
Gambar 4. 12. *Confusion Matrix* Dataset CSIC pada Pengujian Rasio 80:20.... 66
Gambar 4. 13. Hasil Evaluasi ECML Sesi Terbaik Rasio 75:25..... 68
Gambar 4. 14. *Confusion Matrix* Dataset ECML pada Pengujian Rasio 75:25.. 68
Gambar 4. 15. Hasil Evaluasi CSIC Sesi Terbaik Rasio 75:25..... 69
Gambar 4. 16. *Confusion Matrix* Dataset CSIC pada Pengujian Rasio 75:25.... 69
Gambar 4. 17. Hasil Evaluasi ECML Sesi Terbaik *w* 1.0 72
Gambar 4. 18. *Confusion Matrix* Dataset ECML pada Pengujian *w* 1..... 72
Gambar 4. 19. Hasil Evaluasi CSIC Sesi Terbaik *w* 1.0 73

`

Gambar 4. 20. *Confusion Matrix* Dataset CSIC pada Pengujian *w* 1.....74
Gambar 4. 21. Hasil Evaluasi ECML Sesi Terbaik *w* 1.5 75
Gambar 4. 22. *Confusion Matrix* Dataset ECML pada Pengujian *w* 1.5.....75
Gambar 4. 23. Hasil Evaluasi ECML Sesi Terbaik *w* 1.5 76
Gambar 4. 24. *Confusion Matrix* Dataset CSIC pada Pengujian *w* 1.5.....77
Gambar 4. 25. Hasil Evaluasi ECML Sesi Terbaik *c1* 2 79
Gambar 4. 26. *Confusion Matrix* Dataset ECML pada Pengujian *c1* 2.....80
Gambar 4. 27. Hasil Evaluasi CSIC Sesi Terbaik *c1* 2 81
Gambar 4. 28. *Confusion Matrix* Dataset CSIC pada Pengujian *c1* 2.....81
Gambar 4. 29. Hasil Evaluasi ECML Sesi Terbaik *c1* 3 83
Gambar 4. 30. *Confusion Matrix* Dataset ECML pada Pengujian *c1* 3.....83
Gambar 4. 31. Hasil Evaluasi CSIC Sesi Terbaik *c1* 3 84
Gambar 4. 32. *Confusion Matrix* Dataset CSIC pada Pengujian *c1* 3.....84
Gambar 4. 33. Hasil Evaluasi ECML Sesi Terbaik *c2* 2 87
Gambar 4. 34. *Confusion Matrix* Dataset ECML pada Pengujian *c2* 2.....87
Gambar 4. 35. Hasil Evaluasi CSIC Sesi Terbaik *c2* 2 88
Gambar 4. 36. *Confusion Matrix* Dataset CSIC pada Pengujian *c2* 2.....88
Gambar 4. 37. Hasil Evaluasi ECML Sesi Terbaik *c2* 3 90
Gambar 4. 38. *Confusion Matrix* Dataset ECML pada Pengujian *c2* 3.....90
Gambar 4. 39. Hasil Evaluasi CSIC Sesi Terbaik *c2* 3 91
Gambar 4. 40. *Confusion Matrix* Dataset CSIC pada Pengujian *c2* 3.....91
Gambar 4. 41. Hasil Evaluasi ECML Sesi Terbaik Pengujian Kelima 93
Gambar 4. 42. *Confusion Matrix* Dataset ECML pada Pengujian Kelima.....94
Gambar 4. 43. Hasil Evaluasi CSIC Sesi Terbaik Pengujian Kelima 95
Gambar 4. 44. *Confusion Matrix* Dataset CSIC pada Pengujian Kelima.....95
Gambar 4. 45. Hasil Evaluasi ECML dengan SVM 96
Gambar 4. 46. Hasil Evaluasi CSIC dengan SVM.....97
Gambar 4. 47. Grafik Kecepatan Deteksi 99

`

DAFTAR PSEUDOCODE

Pseudocode 1. *Parsing* XML ke JSON 39
Pseudocode 2. *Parsing* TXT ke JSON 41
Pseudocode 3. Panjang Permintaan HTTP 43
Pseudocode 4. Panjang *Query* 44
Pseudocode 5. Panjang *Header* 45
Pseudocode 6. Panjang *Header Content-Length* 45
Pseudocode 7. Jumlah Query 46
Pseudocode 8. Panjang Angka pada *Query* dan *Body* 46
Pseudocode 9. Panjang Angka pada *Path* 47
Pseudocode 10. Panjang Spesial Karakter pada *Query*, *Body*, dan *Path* 47
Pseudocode 11. Panjang Huruf pada *Query*, *Body*, dan *Path* 48
Pseudocode 12. Jumlah *Body* 49
Pseudocode 13. Panjang *Path* 50
Pseudocode 14. Metode *Request* 50
Pseudocode 15. Jumlah Keyword Mencurigakan pada Query, Body, dan Path .. 51
Pseudocode 16. Hitung *Entropy Request* 52
Pseudocode 17. Normalisasi Data dengan *Min-Max Scaling* 53
Pseudocode 18. *Particle Swarm Optimization* (PSO) 54
Pseudocode 19. *Sequalize Minimize Optimize* 55
Pseudocode 20. SVM *Prediction Function* 57
Pseudocode 21. *Fitness Function* Akurasi 58
Pseudocode 22. Deteksi *Hybrid* 59

`

Halaman ini sengaja dikosongkan