MULTI-CLASSIFICATION SERANGAN SIBER MENGGUNAKAN METODE SUPPORT VECTOR MACHINE (SVM)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

oleh
Yahadi Rasyid Albaqi
09011282025060

Fakultas Ilmu komputer
Jurusan Sistem Komputer
Universitas Sriwijaya
2024

HALAMAN PENGESAHAN

MULTI-CLASSIFICATION SERANGAN SIBER MENGGUNAKAN METODE SUPPORT VECTOR MACHINE (SVM)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

oleh
Yahadi Rasyid Albaqi
09011282025060

Indralaya, April 2024

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing,
Dr.Ir.Sukemi,M.T.	**Ahmad Heryanto,S.Kom,M.T.**
NIP.196612032006041001	**NIP.198701222015041002**

AUTHENTICATION PAGE

MULTI-CLASSIFICATION CYBER ATTACK USING SUPPORT VECTOR MACHINE (SVM) METHOD

THESIS

Submitted To Fulfill One Of He Requirement To

Obten A Bachelor's In Computer Science

By

Yahadi Rasyid Albaqi

09011282025060

Indralaya, April 2024

Acknowledge,

Head Of Computer System Department	Pembimbing
Dr.Ir.Sukemi,M.T.	**Ahmad Heryanto,S.Kom,M.T.**
NIP.196612032006041001	**NIP.198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Kamis

Tanggal : 04 April 2024

Tim Penguji :

1. Ketua : Dr. Rossi Passarella,M.Eng.

2. Sekretaris : Nurul Afifah,M.Kom.

3. Penguji : Dr. Ahmad Zarkasi,M.T.

4. Pembimbing : Ahmad Heryanto,S.Kom., M.T.

Mengetahui, 05/5/24

Ketua Jurusan Sistem Komputer

Dr.Ir.Sukemi,M.T.

NIP.196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Yahadi Rasyid Albaqi

NIM : 09011282025060

Judul : Multi-classification Serangan Siber Menggunakan Metode Support Vector Machine (SVM)

Hasil pengecekan Software Itheticate/Turnitin : 5%

Menyatakan bahwa laporan tugas akhir sata merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan

Indralaya, April 2024

Yahadi Rasyid Albaqi

09011282025060

KATA PENGANTAR

Asslaamualaikum Warahmatuallahi Wabarakatuh

Puji syukur Alhamdulillah kepada Allah SWT yang telah memberikan ridho dan berkah-Nya, sehingga penulis dapat menyelesaikan penyusunan Laporan Tugas Akhir yang berjudul " *Multi-classification* Serangan Siber Menggunakan Metode *Support Vector Machine* (SVM)".

Pada penyusunan laporan ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan mengucapkan banyak terima kasih kepada :

1. Allah SWT yang telah memberikan saya berkat dan rahmat-Nya serta kesehatan untuk menyelesaikan laporan tugas akhir ini.
2. kepada orang tua, kakak dan ayuk yang saya cintai karena telah memberika doa dan motivasi kepada penulis.
3. Bapak Pof.Dr. Erwin,S.Si M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr.Ir. H. Sukemi,M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Rahmat Fadli Isnanto,S.Kom. M.SC. selaku Dosen Pembimbing Akademik
6. Bapak Ahmad Heryanto,S.Kom. M.T. selaku Dosen Pembimbing Skripsi yang telah meluangkan waktu untuk membimbing serta memberikan saran dan motivasi terbaik.
7. Administrasi Jurusan Sistem Komputer yang telah membantu dan melancarkan proses administrasi terkait Tugas Akhir.
8. Muhammad Indra, M.pd dan Tika Felandari, S.Sos yang telah membantu dan membimbing peneliti dalam pengerjaan skripsi ini.
9. Kepada teman kelas SKB 2020 dan teman di lab comnets yang sudah memberikan bantuan.
10. Kakak tingkat Jurusan Sistem Komputer Universitas Sriwijaya yang Telah memberikan bantuan nya.

11 Dan seluruh pihak yang tidak dapat penuli sebutkan yang selalu memberikan semangat dan bantun yang bermanfaat

Penulis Menyadari bahwa laporan ini masih banyak kekurangan Oleh karena itu penulis mengharapkan kritik dan saran dari semua pihak sebagai bahan evaluasi dari penulis agar laporan ini menjadi lebih baik dan bermanfaat bagi semua pihak dan menjadi referensi bacaan dalam penelitian networking terkhusus pada serangan siber

Wassalamualaikum Warahatullahi Wabarakatuh

Palembang, Februari

Penulis,

Yahadi Rasyid Albaqi

NIM.09011282025060

MULTI-CLASSIFICATION OF CYBER ATTACKS USING SUPPORT VECTOR MACHINE (SVM) METHOD

YAHADI RASYID ALBAQI (09011282025060)

Department of Computer Systems, Faculty of Computer Science, Sriwijaya University

Email : yahadialbaqi25@gmail.com

ABSTRACT

Cyberattacks are unauthorized attempts to track and disrupt the operation of communication systems and control systems by exploiting the security weaknesses of communication networks. Efforts to protect these systems can be made using multi-classification. Multi-classification is a classification that can understand the relationship between cyber-attacks so as to increase the ability of recognition and overcome the limitations related to classification. The method used in this research is Support Vector Machine (SVM) using the *One Against one-SVM*(OAO-SVM) and *One against All-SVM*(OAA-SVM) approaches so that the research results can be compared regarding accuracy and computing time. This research uses four types of datasets namely CSE-CIC-IDS2018, ISCXIDS2012, NSL-KDD, and KDD CUP 1999. By using validation on training and testing data from 20% to 80%. So that the best results were obtained on the CSE-CIC-IDS2018, ISCXIDS2012, and KDD CUP 1999 datasets using the SVM method with accuracy of 99.18%, 99.82%, and 99.92%. Then using the OAO-SVM method on the NSL-KDD dataset with the accuracy obtained is 99.66% with more efficient computing time on each dataset used. While the OAA-SVM method has lower accuracy with longer computation time.

Keywords: *Cyber Attack, Multi-Classification, Support Vector Machine (SVM), One Against One-SVM (OAO-SVM), One Against All-SVM (OAA-SVM).*

Acknowledge,

Head of Computer System Department	**Supervisor**
Dr.Ir.Sukemi,M.T.	**Ahmad Heryanto,S.Kom,M.T.**
NIP.196612032006041001	**NIP.198701222015041002**

MULTI-CLASSIFICATION SERANGAN SIBER MENGGUNAKAN METODE SUPPORT VECTOR MACHINE (SVM)

YAHADI RASYID ALBAQI (09011282025060)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : yahadialbaqi25@gmail.com

ABSTRAK

Serangan siber merupakan upaya tidak sah untuk melacak dan mengganggu operasi sistem komunikasi dan sistem kontrol dengan memanfaatkan kelemahan keamanan jaringan komunikasi. Upaya untuk melindungi sistem tersebut dapat dilakukan menggunakan multi-classification. Multi-clasification adalah klasifikasi yang dapat memahami hubungan antara serangan siber sehinga meningkatkan kemapuan pengenalam dan mengatasi batasan-batasan terkait klasifikasi. Metode yang digunakan dalam penelitian ini ialah Support Vector Machine(SVM) dengan menggunakan pendekatan *One Against one*-SVM(OAO-SVM) dan *One against All*-SVM(OAA-SVM) sehingga hasil penelitian dapat dibandingkan terkait akurasi dan komputasi waktu. Penelitian ini menggunakan empat jenis dataset yaitu CSE-CIC-IDS2018, ISCXIDS2012, NSL-KDD, dan KDD CUP 1999. Dengan menggunakan validasi pada data training dan testing dari 20% sampai 80%. Sehingga diperoleh hasil terbaik pada dataset CSE-CIC-IDS2018, ISCXIDS2012, dan KDD CUP 1999 menggunakan metode SVM dengan akurasi yaitu 99,18%, 99,82%, dan 99,92%. Kemudian dengan menggunakan metode OAO-SVM pada dataset NSL-KDD dengan akurasi yang diperoleh yaitu 99,66% dengan waktu komputasi yang lebih efisien pada setiap dataset yang digunakan. Sedangkan pada metode OAA-SVM memiliki akurasi yang lebih rendah dengan waktu komputasi yang lebih lama.

Kata kunci : *Serangan Siber, Multi-Classification, Support Vector Machine (SVM), One Against One-SVM (OAO-SVM), One Against All-SVM (OAA-SVM).*

Acknowledge,

Head of Computer System Department	**Supervisor**
Dr.Ir.Sukemi,M.T.	**Ahmad Heryanto,S.Kom,M.T.**
NIP.196612032006041001	**NIP.198701222015041002**

DAFTAR ISI

HALAMAN PENGESAHAN ..... **ii**

AUTHENTICATION PAGE ..... **iii**

HALAMAN PERSETUJUAN ..... **iv**

HALAMAN PERNYATAAN ..... **v**

KATA PENGANTAR ..... **vi**

ABSTRAK ..... **viii**

ABSTRACT ..... **ix**

DAFTAR ISI ..... **x**

DAFTAR GAMBAR ..... **xiv**

DAFTAR TABEL ..... **xvii**

BAB 1 Pendahuluan **1**

1.1 Latar Belakang 1

1.2 Perumusan Masalah 4

1.3 Tujuan 4

1.4 Manfaat 5

1.5 Batasan masalah 5

1.6 Sistematika Penelitian 5

BAB II Tinjauan Pustaka **7**

2.1 Penelitian Terkait 7

2.2 Penelitian Terdahulu/penelitian terkait/state of the art 14

2.3 Serangan Siber 20

2.3.1 Daniel of Service (DoS) 21

2.3.2 Distributed Daniel of Service (DDoS) 21

2.3.3 Botnet 21

2.3.4 Brute Force 22
2.3.5 Infiltring Network from Inside 22
2.3.6 Serangan Probing (Probing Attack) 22
2.3.7 Serangan U2R(User to Root) 23
2.3.8 Serangan URL(URL Attack) 23
2.3.9 Serangan R2L(Remote to local) 23
2.4 Multi-classification 24
2.5 Support Vector Mechine(SVM) 25
2.6 One Against One-Support Vector Machine(OAO-SVM) 27
2.7 One Against All-Suppor Vector Machine (OAA-SVM) 29
2.8 Kernel Support Vector Machine 30
2.9 Confusion matrix 31
2.9.1 Akurasi 32
2.9.2 Recall 32
2.9.3 Spesifitas 32
2.9.4 Presisi 33
2.9.5 F1-Score 33
BAB III METODOLOGI PENELITIAN 34
3.1 Diagram Alir Penelitian 34
3.2 Tahap Persiapan 36
3.3 Kerangka kerja metodologi Penelitian 37
3.4 Perangkat dan Aplikasi 38
3.4.1 Perangkat Keras(Hardware) 38
3.4.2 Peragkat Lunak(Software) 38
3.5 Dataset 39
3.5.1 Dataset CSE CIC-IDS 2018 39

3.5.2 ISCXIDS 2012 47
3.5.3 Dataset NSL-KDD 49
3.5.4 KDD CUP 1999 54
3.6 Pre-Processing Dataset 57
3.7 Fitur Seleksi 61
3.8 Metode Support Vector Machine 62
3.8.1 Arsitektur Support Vector Machine(SVM) 71
3.8.2 Arsitektur One Against One Support Vector Machine 72
3.8.3 Arsitektur One Against All Support Vector Machine 73
3.9 Validasi Hasil 74
3.9.1 Pengujian Hyperparameter CSE-CIC-IDS2018 76
3.9.2 Pengujian Hyperparameter ISCXIDS2012 77
3.9.3 Pengujian Hyperparameter NSL-KDD 80
3.9.4 Pengujian Hyperparameter KDD CUP 1999 81
BAB IV HASIL DAN ANALISIS 84
4.1 Seleksi Fitur 84
4.1.1 Seleksi Fitur Dataset CSE CIC-IDS2018 85
4.1.2 Seleksi Fitur Dataset ISCXIDS2012 88
4.1.3 Seleksi Fitur Dataset NSL-KDD 90
4.1.4 Fitur Seleki dari Dataset KDD-CUP1999 93
4.2 Penggunaan SMOTE Pada Dataset 96
4.3 Pengelompokkan dataset berupa data training dan data testing 103
4.4 Validasi Hasil 103
4.4.1 Validasi Hasil pada Dataset CSE-CIC-IDS2018 104
4.4.2 Validasi Hasil pada Dataset ISCXIDS2012 118
4.4.3 Validasi Hasil pada Dataset NSL-KDD 132

4.4.4 Validasi Hasil pada Dataset KDD CUP 1999 146
4.5 Cross Validation 160
4.5.1 Cross Validation Dataset CSE-CIC-IDS2018 160
4.5.2 Cross Validation Dataset ISCXIDS2012 161
4.5.3 Cross Validation Dataset NSL-KDD 163
4.5.4 Cross Validation Dataset KDD CUP 1999 164
4.6 Analisa Hasil Penelitian 166
4.7 Perbandingan Terhadap Penelitian Terdahulu 173
BAB V KESIMPULAN DAN SARAN 175
5.1 Kesimpulan 175
5.2 Saran 176
DAFTAR PUSTAKA 177
LAMPIRAN 184

DAFTAR GAMBAR

Gambar 2. 1 Penerapan Multi-classification 24
Gambar 2. 2 Hyperplane SVM 26
Gambar 2. 3 OAO-SVM 27
Gambar 2. 4 OAA-SVM 29
Gambar 2. 5 Confusion matrix 31
Gambar 3. 1 Diagram Alir Penelitian 35
Gambar 3. 2 Tahap Persiapan 36
Gambar 3. 3 Pengecekan data duplikat 58
Gambar 3. 4 Label Encoder 59
gambar 3. 5 Missing Value 60
Gambar 3. 6 Fitur Seleksi 61
Gambar 3. 7 Struktur SVM 62
Gambar 3. 8 Hyperplane Margin Maksimum 63
Gambar 3. 9 Kerangka Kerja Klasifikasi Menggunakan SVM 64
Gambar 3. 10 Import Library 65
Gambar 3. 11 Train test split pada SVM 66
Gambar 3. 12 Standar Scaler pada SVM 68
Gambar 3. 13 Model.fit klasifikasi 69
Gambar 3. 14 Model Predict 70
Gambar 3. 15 Arsitektur Support Vector Machine 71
Gambar 3. 16 Arsitektur One Against One Support Vector Machine 72
Gambar 3. 17 Arsitektur One Against All Support Vector Machine 73
Gambar 3. 18 Flowchart Validasi Hasil 75
Gambar 4. 1 Grafik Korelasi Dataset CSE-CIC-IDS2018 85
Gambar 4. 2 Grafik Korelasi dari Dataset ISCXIDS2012 88
Gambar 4. 3 Grafik Korelasi dari Dataset NSL-KDD 90
Gambar 4. 4 Grafik Korelasi dari Dataset KDD CUP 1999 93
Gambar 4. 5 Grafik Unbalanced Dataset CSE-CIC-IDS2018 96
Gambar 4. 6 Grafik SMOTE Dataset CSE-CICIDS2018 97
Gambar 4. 7 Grafik Unbalanced Dataset ISCXIDS2012 98

Gambar 4. 8 Grafik SMOTE Dataset ISCXIDS2012 98
Gambar 4. 9 Grafik Unbalanced Dataset NSL-KDD 99
Gambar 4. 10 Grafik SMOTE Dataset NSL-KDD 100
Gambar 4. 11 Grafik Unbalanced Dataset KDD CUP 1999 101
Gambar 4. 12 Grafik SMOTE Dataset KDD CUP 1999 102
Gambar 4. 13 Pembagian data training dan data testing 103
Gambar 4. 14 Average Presisi score Metode SVM CSE-CIC-IDS2018 107
Gambar 4. 15 Grafik presisi-recall Metode SVM CSE-CIC-IDS2018 108
Gambar 4. 16 Grafik ROC Metode SVM CSE-CIC-IDS2018 109
Gambar 4. 17 Average Presisi score OAO-SVM CSE-CIC-IDS2018 111
Gambar 4. 18 Grafik presisi-recall Metode OAO-SVM CSE-CIC-IDS2018 .. 112
Gambar 4. 19 Grafik ROC Metode OAO-SVM CSE-CIC-IDS2018 113
Gambar 4. 20 Average Presisi score Metode OAA-SVM CSE-CIC-IDS2018. 115
Gambar 4. 21 Grafik presisi-recall Metode OAA-SVM CSE-CIC-IDS2018 .. 116
Gambar 4. 22 Grafik ROC Metode OAA-SVM CSE-CIC-IDS2018 117
Gambar 4. 23 Average Presisi score Metode SVM ISCXIDS2012 121
Gambar 4. 24 Grafik presisi-recall Metode SVM ISCXIDS2012 122
Gambar 4. 25 Grafik ROC Metode SVM ISCXIDS2012 123
Gambar 4. 26 Average Presisi score Metode OAO-SVM ISCXIDS2012 125
Gambar 4. 27 Grafik presisi-recall Metode OAO-SVM ISCXIDS2012 126
Gambar 4. 28 Grafik ROC Metode OAO-SVM ISCXIDS2012 127
Gambar 4. 29 Average Presisi score Metode OAA-SVM ISCXIDS2012 129
Gambar 4. 30 Grafik presisi-recall Metode OAA-SVM ISCXIDS2012 130
Gambar 4. 31 Grafik ROC Metode OAA-SVM ISCXIDS2012 131
Gambar 4. 32 Average Presisi score Metode SVM NSL-KDD 135
Gambar 4. 33 Grafik presisi-recall Metode SVM NSL-KDD 136
Gambar 4. 34 Grafik ROC Metode SVM NSL-KDD 137
Gambar 4. 35 Average Presisi score Metode OAO-SVM NSL-KDD 139
Gambar 4. 36 Grafik presisi-recall Metode OAO-SVM NSL-KDD 140
Gambar 4. 37 Grafik ROC Metode OAO-SVM NSL-KDD 141
Gambar 4. 38 Average Presisi score Metode OAO-SVM NSL-KDD 143
Gambar 4. 39 Grafik presisi-recall Metode OAA-SVM NSL-KDD 144

Gambar 4. 40 Grafik ROC Metode OAA-SVM NSL-KDD 145
Gambar 4. 41 Average Presisi score Metode SVM KDD CUP 1999 149
Gambar 4. 42 Grafik presisi-recall Metode SVM KDD CUP 1999..... 150
Gambar 4. 43 Grafik ROC Metode SVM Dataset KDD CUP 1999 151
Gambar 4. 44 Average Presisi score Metode OAO-SVM KDD CUP 1999 153
Gambar 4. 45 Grafik presisi-recall Metode OAO-SVM Dataset 154
Gambar 4. 46 Grafik ROC Metode OAO-SVM KDD CUP 1999 155
Gambar 4. 47 Average Presisi score Metode OAA-SVM KDD CUP 1999 157
Gambar 4. 48 Grafik presisi-recall Metode OAO-SVM KDD CUP 1999..... 158
Gambar 4. 49 Grafik ROC Metode OAO-SVM KDD CUP 1999 159
Gambar 4. 50 Grafik Cross Validation Dataset CSE-CIC-IDS2018..... 161
Gambar 4. 51 Grafik Cross Validation Dataset ISCXIDS2012 163
Gambar 4. 52 Grafik Cross Validation Dataset NSL-KDD 164
Gambar 4. 53 Grafik Cross Validation Dataset KDD CUP 1999 166
Gambar 4. 54 Visualisasi Performa dataset CSE-CIC-IDS2018..... 170
Gambar 4. 55 Visualisasi Performa Pengujian pada dataset ISCXIDS2012..... 170
Gambar 4. 56 Visualisasi Performa Pengujian pada dataset NSL-KDD..... 171
Gambar 4. 57 Visualisasi Performa Pengujian pada dataset KDD CUP 1999.. 171

DAFTAR TABEL

Tabel 2. 1 Penelitian Terkait 7
Tabel 3. 1 Hardware yang digunakan 38
Tabel 3. 2 Software yag digunakan 38
Tabel 3. 3 Fitur-fitur dataset CSE-CIC-IDS 2018 40
Tabel 3. 4 Fitur- Fitur Dataset ISCXIDS2012 47
Tabel 3. 5 Fitur-Fitur Dataset NSL-KDD 49
Tabel 3. 6 Fitur-Fitur Dataset KDD CUP 1999 54
Tabel 3. 7 Hasil percobaan parameter kernel CSE CIC IDS 2018 76
Tabel 3. 8 Hasil Pengujian Pada Parameter C 76
Tabel 3. 9 Hasil Pengujian Pada Parameter tolerance 77
Tabel 3. 10 Hasil pengujian parameter kernel ISCXIDS2012 77
Tabel 3. 11 Hasil Pengujian Pada Parameter C 78
Tabel 3. 12 Hasil Pengujian pada parameter Degree 78
Tabel 3. 13 Hasil Pengujian pada parameter Coef0 79
Tabel 3. 14 Hasil percobaan parameter kernel pada dataset NSL-KDD 80
Tabel 3. 15 Hasil Pengujian Pada Parameter C 80
Tabel 3. 16 Hasil Pengujian Pada Parameter Gamma 81
Tabel 3. 17 Hasil percobaan parameter kernel pada dataset KDD CUP 1999 81
Tabel 3. 18 Hasil Pengujian Pada Parameter C 82
Tabel 3. 19 Hasil Pengujian pada Parameter Gamma 82
Tabel 3. 20 Penggunaan Hyperparameter 83
Tabel 3. 21 Pembagian Jumlah data 83
Tabel 4. 1 Nilai Korelasi Fitur Dataset CSE-CICIDS2018 86
Tabel 4. 2 Nilai Korelasi Fitur Dataset ISCXIDS2012 89
Tabel 4. 3 Nilai Korelasi Fitur Dataset NSL-KDD 91
Tabel 4. 4 Nilai Korelasi Fitur dari Dataset KDD CUP 1999 94
Tabel 4. 5 Hasil Validasi dataset CSE-CIC-IDS2018 104
Tabel 4. 6 klasifikasi perhitungan Metode SVM CSE-CIC-IDS2018 106
Tabel 4. 7 klasifikasi perhitungan Metode OAO-SVM CSE-CIC-IDS2018 110
Tabel 4. 8 klasifikasi perhitungan Metode OAA-SVM CSE-CIC-IDS2018 114
Tabel 4. 9 Hasil Validasi dataset ISCXIDS2012 118

Tabel 4. 10 klasifikasi perhitungan Metode SVM ISCXIDS012 120
Tabel 4. 11 klasifikasi perhitungan Metode OAO-SVM ISCXIDS2012 124
Tabel 4. 12 klasifikasi perhitungan Metode OAA-SVM ISCXIDS2012 128
Tabel 4. 13 Hasil Validasi dataset NSL-KDD 132
Tabel 4. 14 klasifikasi perhitungan Metode SVM NSL-KDD 134
Tabel 4. 15 Klasifikasi perhitungan Metode OAO-SVM NSL-KDD 138
Tabel 4. 16 klasifikasi perhitungan Metode OAA-SVM NSL-KDD 142
Tabel 4. 17 Hasil Validasi dataset KDD-CUP 1999 146
Tabel 4. 18 klasifikasi perhitungan Metode SVM KDD CUP 1999 148
Tabel 4. 19 klasifikasi perhitungan Metode OAO-SVM KDD CUP 1999 152
Tabel 4. 20 Klasifikasi perhitungan Metode OAA-SVM KDD CUP 1999 156
Tabel 4. 21 Hasil Cross Validation Dataset CSE-CIC-IDS2018 160
Tabel 4. 22 Hasil Cross Validation Dataset ISCXIDS2012 162
Tabel 4. 23 Hasil Cross Validation Dataset NSL-KDD 163
Tabel 4. 24 Hasil Cross Validation Dataset KDD CUP 1999 165
Tabel 4. 25 Perbandingan Performa model SVM 169
Tabel 4. 26 Perbandingan Waktu Komputasi 172
Tabel 4. 27 Hasil Perbandingan Terhadap Penelitian Terkait 173

BAB 1
Pendahuluan

1.1 Latar Belakang

Beberapa tahun terakhir, keamanan data menjadi sangat rentan terhadap serangan siber [1]. Serangan siber merupakan upaya tidak sah untuk melacak dan mengganggu operasi sistem komunikasi dan sistem kontrol dengan memanfaatkan kelemahan keamanan jaringan komunikasi [2]. Salah satu contoh serangan siber adalah Dos Attack, DDOS attack, brute force, dan botnet yang dapat merusak sistem [3] [4] [5] [6]. Serangan-serangan ini bertujuan untuk mengakses dan mengambil alih kontrol atas sistem yang diserang sehingga dapat menyebabkan kerugian yang signifikan bagi pihak yang terkena dampaknya.

Terkait Laporan investigasi serangan siber pada tahun 2017, terjadi serangan ransomware yang dikenal dengan nama WannaCry. Serangan ini menargetkan sistem operasi Windows dan memanfaatkan kerentanan pada protokol jaringan. Dalam waktu singkat, serangan ini menyebar dengan cepat dan menginfeksi sejumlah besar komputer di seluruh dunia, termasuk rumah sakit, perusahaan, dan lembaga pemerintah. Penyerang kemudian meminta pembayaran tebusan dalam bentuk *bitcoin* agar akses ke data yang terenkripsi dapat dikembalikan kepada korban [7]. Serangan ini menunjukkan tingkat penyebaran yang sangat luas dan berdampak signifikan pada berbagai sektor, memaksa banyak organisasi untuk menghadapi konsekuensi serius.

Menghadapi jenis serangan siber yang semakin beragam, dibutuhkan pembelajaran mesin atau *supervised learning* yang mampu mempelajari pola dari data yaitu *multi-classification*[8] . *Multi-classification* dapat mengelompokkan data ke dalam beberapa kelas yang berbeda sehingga memungkinkan representasi yang lebih akurat dan komprehensif [9] [10]. Pada data yang kompleks seperti serangan siber, *multi-classification* dapat memperoleh pemahaman yang lebih mendalam tentang hubungan antara kategori-kategori, meningkatkan kemampuan pengenalan ,dan mengatasi batasan-batasan yang terkait dengan klasifikasi *non multi-classification*. Sedangkan pada classification *non multi-classification* atau *binery classification* terdapat masalah yang timbul yaitu keterbatasan reperesentasi, keputusan yang ambigu,dan terjadi kehilangan informasi yang penting [11]

Analisis serangan siber pada data yang kompleks dan beragam memerlukan penggunaan *multi-classification* untuk memahami hubungan antara jenis serangan siber. Adapun metode yang efektif untuk menerapkan *multi-classification* adalah *Support Vector Machine* (SVM). Hal ini sejalan dengan hasil penelitian dari [12] yang meyatakan algoritma klasifikasi SVM efektif mendeteksi serangan siber. Serangan siber yang dideteksi membandingkan dataset NSL-KDD dan KDD-CUP pada 2 kelas, 5 kelas, dan 13 kelas klasifikasi menggunakan penilaian kurva AUC *(Area Under Curve)*. Penelitian tersebut memperoleh hasil akurasi pada 2 kelas klasifikasi dataset NSL-KDD yaitu 0.85 sedangkan pada dataset KDD-CUP 99 yaitu 0,86 . Penelitian pada 5 kelas klasifikasi memperoleh hasil akurasi 0,77% sedangakan pada dataset KDD-CUP yaitu 0,92. Terakhir pada 13 kelas klasifikasi menggunakan dataset NSL-KDD memperoleh hasil akurasi 0,89%.

Support Vector Machine (SVM) adalah algoritma pembelajaran mesin yang bekerja dengan mencari *Hyperplane* terbaik dengan mengklasifikasikan data ke dalam kelas-kelas secara optimal [13]. SVM mampu membedakan serta memisahkan antara data serangan dan data normal dengan cara pembagian antar *class*. Kelebihan dari SVM adalah kemampuanya untuk mengklasifikasikan dataset dengan banyak fitur *(high-dimensional)* dan jumlah sampel yang retatif kecil. Selain itu, SVM memiliki kemampuan untuk mengklasifikasikan data yang tidak seimbang *(imbalanced data)*. Pada penelitian [14] menyatakan bahwa dengan menggunakan metode SVM mampu menghasilkan akurasi sebesar 94%. Hal ini juga sejalan dengan penelitian dari [15] yang menyebutkan tingkat akurasi metode SVM dalam klasifikasi adalah 99,85%.

Karakteristik dari metode *Support Vector Machine* (SVM) adalah SVM mencari *Hyperplane* terbaik yang dapat memisahkan kelas-kelas yang berbeda dalam data. *Hyperplane* ini berfungsi untuk membedakan antara data dari kelas yang berbeda. Selanjutnya, SVM berupaya mencari *Hyperplane* dengan *margin* terbesar di antara kelas-kelas tersebut. *Margin* adalah jarak antara *Hyperplane* dan titik data terdekat dari setiap kelas. Dengan memaksimalkan *margin*, SVM dapat memiliki ketahanan yang lebih baik terhadap data yang tidak terlihat sebelumnya, sehingga dapat menghasilkan akurasi yang lebih baik dalam klasifikasi multi-kelas [16]. Dalam Metode *Support Vector Machine* (SVM), *multi-classification* mengacu

pada kasus di mana terdapat lebih dari dua kelas yang harus diklasifikasikan. Pendekatan yang digunakan untuk klasifikasi tersebut adalah dengan pendekatan *One Against One* (OAO) dan *One Against All* (OAA).

Dalam pendekatan *One Against One* (OAO), SVM melatih beberapa model SVM yang membandingkan setiap pasangan kelas secara terpisah. Jika terdapat N kelas, maka akan ada N*(N-1)/2 model SVM yang dilatih [17] [18]. Berdasarkan penelitian yang dilakukan oleh [19] menyatakan bahwa klasifikasi OAO-SVM yang dikombinasikan dengan fitur reduksi berhasil meningkatkan kinerja sistem. Klasifiasi dilakuakn dengan cara memecahkan masalah kategori profil multi-kelas setiap model SVM dibentuk untuk membedakan satu kelas dari yang lain. Saat ada data baru yang perlu diklasifikasikan, model-model SVM ini akan memberikan suara atau voting berdasarkan hasil klasifikasi. kelas dengan suara terbanyak akan dipilih sebagai prediksi akhir Kombinasi.

Dalam pendekatan *One Against All* (OAA), SVM melatih model SVM terhadap setiap kelas secara terpisah dan menganggap kelas tersebut sebagai kelas positif, sementara kelas lainnya dianggap sebagai kelas negatif. Dalam kasus ini, jika terdapat N kelas, maka akan ada N model SVM yang dilatih. Setiap model SVM akan membedakan satu kelas dari semua kelas lainnya. Berdasarkan penelitian terdahulu yang telah diteliti menyatakan bahwa pendeketan OAA-SVM terbukti efektif dalam multiclass-classification dengan dikombinasikan menggukan teknik yang dicoba [17] [18] [20]. OAA-SVM mampu mengidentifikasi kesalahan gabungan tunggal dan ganda pada bantalan kecepatan rendah. Hasil percobaan menunjukkan bahwa teknik pengklasifikasi lebih unggul dibandingkan algoritma lain, dengan peningkatan 6,19 – 16,59% kinerja klasifikasi rata-rata [21].

Berdasarkan pemaparan di atas, maka peneliti tertarik mengambil judul "***Multi-classification* Serangan Siber Menggunakan Metode *Support Vector Machine* (SVM) "**. Dimana keunggulan dari metode ini mampu mengklasifikasikan dataset dengan fitur yang beragam dan tidak seimbang. Selain itu, metode SVM yang digunakan akan dikombinasikan menggunakan teknik yang telah diuji pada penelitian sebelumnya. Sehingga memberikan akurasi sistem *multi-classification* serangan siber yang lebih efektif dan efisien.

1.2 Perumusan Masalah

Perumusan masalah berdasarkan hasil pada latar belakang yang telah dikemukakan, antara lain:

1. Bagaimana pengaruh efektivitas penggunanaan metode SVM dalam *multi-classification*serangan siber ?
2. Bagaimana cara kerja CFS dalam menghasilkan Fitur Terbaik untuk klasifikasi serangan siber ?
3. Bagaimana Perbandingan akurasi serangan siber menggunakan metode *Support Vector Machine* (SVM), metode *One Against One*-SVM (OAO-SVM) dan *One Against All*-SVM(OAA-SVM) ?
4. Bagaimana Perbandingan waktu komputasi serangan siber menggunakan Metode *Support Vector Machine* (SVM), Metode *One Against One*-SVM (OAO-SVM) dan Metode *One Against All*-SVM(OAA-SVM) ?

1.3 Tujuan

Tujuan dari penelitian ini, antara lain :

1. Merancang sistem *multi-classification* serangan siber pada jaringan komputer yang efektif dan dapat mengidentifikasi berbagai jenis serangan siber.
2. Melakukan seleksi fitur pada setiap dataset agar memperoleh fitur terbaik dari korelasi pada setiap fitur yang memiliki kesamaan.
3. Membandingkan metode SVM, OAO-SVM, dan OAA-SVM dalam sistem *multi-classification*untuk memperoleh akurasi yang paling efektif dalam sistem *multi-classification*serangan siber.
4. Melakukan evaluasi kinerja sistem *multi-classification*untuk membandingkan watu komputasi metode SVM, OAO-SVM, dan OAA-SVM.

1.4 Manfaat

Manfaat dari penelitian ini, antara lain :

1. Memberikan pemahaman yang lebih baik tentang serangan siber dan teknik-teknik yang dapat digunakan untuk mendeteksinya pada jaringan komputer.
2. Mengembangkan sistem deteksi serangan siber yang efektif dan dapat membantu melindungi jaringan komputer dari serangan yang merugikan.
3. Menerapkan metode *Support Vector Machine* (SVM) dalam sistem deteksi *multi-classification*, yang dapat meningkatkan akurasi dalam mendeteksi serangan siber pada jaringan komputer.

1.5 Batasan masalah

Batasan Masalah yang didapatkan pada penelitian tugas akhir yaitu seperti di bawah ini :

1. Pada penelitian ini menggunaan dataset CSE-CIC-IDS2018, ISCX2012, NSL-KDD, dan KDD CUP 1999.
2. Metode yang digunakan menggunakan algoritma *Support Vector Machine* (SVM) dengan bahasa pemrograman python.
3. Nilai parameter yang diteliti akan dijadikan sebagai output dari penelitian ini berupa nilai dari akurasi, nilai dari recall, nilai dari spesifisitas, nilai dari presisi, nilai F1-Score.

1.6 Sistematika Penelitian

Penelitian yang digunakan oleh peneliti pada tugas akhir ini, antara lain:

BAB I PENDAHULUAN

Bab bagian pertama berisikan paparan secara sistematis dari latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab tugas akhir bagian kedua berisikan penjelasan teori dasar yang menunjang penelitian ini. Dasar teori tersebut membahas literatur terhadap membahas konsep dasar serangan siber, *multi-classification*, metode SVM, OAO-SVM, OAA SVM, *Confusion matrix*.

BAB III METODOLOGI PENELITIAN

Bab penelitian bagian ketiga ini menjelaskan bagaimana proses saat menjalankan penelitian, dimulai dari tahap persiapan data, pengolahan data, ekstraksi fitur, pembagian data latih dan uji dengan beberapa *Hyperparameter* dan validasi performa.

BAB IV HASIL DAN PEMBAHASAN

Bab bagian empat pada penelitian ini menjelaskan hasil dan analisa akhir dari penelitian yang telah dilakukan sebelumnya oleh peneliti. Di bagian ini, peneliti akan memaparkan hasil percobaan, evaluasi model, dan perbandingan terhadap penelitian terdahulu.

BAB V KESIMPULAN

Bab yang kelima ini merupakan bagian kesimpulan berdasarkan perolehan dari hasil dan analisa pada evaluasi pengujian terhadap penelitian telah selesai dilakukan.

DAFTAR PUSTAKA

[1] I. Ullah and Q. H. Mahmoud, "A Two-Level Hybrid Model for Anomalous Activity Detection in IoT Networks," in *2019 16th IEEE Annual Consumer Communications and Networking Conference, CCNC 2019*, Feb. 2019. doi: 10.1109/CCNC.2019.8651782.

[2] H. Zolfi, H. Ghorbani, and M. H. Ahmadzadegan, "Investigation and classification of cyber-crimes through IDS and SVM algorithm," in *Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019*, Dec. 2019, pp. 180–187. doi: 10.1109/I-SMAC47947.2019.9032536.

[3] K. S. Sahoo *et al.*, "An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020, doi: 10.1109/ACCESS.2020.3009733.

[4] A. Kajal and S. K. Nandal, "A hybrid approach for cyber security: Improved intrusion detection system using ann-svm," *Indian J. Comput. Sci. Eng.*, vol. 11, no. 4, pp. 412–425, 2020, doi: 10.21817/indjcse/2020/v11i4/201104300.

[5] S. Salaria, S. Arora, N. Goyal, P. Goyal, and S. Sharma, "Implementation and Analysis of an Improved PCA technique for DDoS Detection," in *2020 IEEE 5th International Conference on Computing Communication and Automation, ICCCA 2020*, Oct. 2020, pp. 280–285. doi: 10.1109/ICCCA49541.2020.9250912.

[6] D. Zhang, D. Tang, L. Tang, R. Dai, J. Chen, and N. Zhu, "PCA-SVM-based approach of detecting low-rate DoS attack," in *Proceedings - 21st IEEE International Conference on High Performance Computing and Communications, 17th IEEE International Conference on Smart City and 5th IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2019*, Aug. 2019, pp. 1163–1170. doi: 10.1109/HPCC/SmartCity/DSS.2019.00164.

[7] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "Ransomware

detection and mitigation using software-defined networking: The case of WannaCry," *Comput. Electr. Eng.*, vol. 76, pp. 111–121, Jun. 2019, doi: 10.1016/j.compeleceng.2019.03.012.

[8] S. Singh, S. V. Fernandes, V. Padmanabha, and P. E. Rubini, "MCIDS-Multi classifier intrusion detection system for IoT cyber attack using deep learning algorithm," in *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, Feb. 2021, pp. 354–360. doi: 10.1109/ICICV50876.2021.9388579.

[9] P. Toupas, D. Chamou, K. M. Giannoutakis, A. Drosou, and D. Tzovaras, "An intrusion detection system for multi-class classification based on deep neural networks," *Proc. - 18th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2019*, pp. 1253–1258, 2019, doi: 10.1109/ICMLA.2019.00206.

[10] A. Mishra, A. M. K. Cheng, and Y. Zhang, "Intrusion Detection Using Principal Component Analysis and Support Vector Mac hines," in *IEEE International Conference on Control and Automation, ICCA*, Oct. 2020, vol. 2020-Octob, pp. 907–912. doi: 10.1109/ICCA51439.2020.9264568.

[11] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection," *IEEE Access*, vol. 6, pp. 33789–33795, May 2018, doi: 10.1109/ACCESS.2018.2841987.

[12] W. Wang, X. Du, D. Shan, R. Qin, and N. Wang, "Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine," *IEEE Trans. Cloud Comput.*, vol. 10, no. 3, pp. 1634–1646, 2022, doi: 10.1109/TCC.2020.3001017.

[13] S. Lysenko, K. Bobrovnikova, O. Savenko, and A. Kryshchuk, *BotGRABBER: SVM-Based Self-Adaptive System for the Network Resilience Against the Botnets' Cyberattacks*, vol. 1039. Springer International Publishing, 2019. doi: 10.1007/978-3-030-21952-9_10.

[14] A. Bachar, N. El Makhfi, and O. El Bannay, "Towards a behavioral

network intrusion detection system based on the SVM model," in *2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology, IRASET 2020, IEEE*, Apr. 2020. doi: 10.1109/IRASET48871.2020.9092094.

[15] R. Vijayanand, D. Devaraj, and B. Kannapiran, "Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection," *Comput. Secur.*, vol. 77, pp. 304–314, Aug. 2018, doi: 10.1016/j.cose.2018.04.010.

[16] P. Tao, Z. Sun, and Z. Sun, "An Improved Intrusion Detection Algorithm Based on GA and SVM," *IEEE Access*, vol. 6, pp. 13624–13631, Mar. 2018, doi: 10.1109/ACCESS.2018.2810198.

[17] A. Iqbal and T. Jain, "Synchrophasor based data driven approach for fault identification using multi-class support vector machine," *2020 21st Natl. Power Syst. Conf. NPSC 2020*, Dec. 2020, doi: 10.1109/NPSC49263.2020.9331920.

[18] A. Eisenmann, T. Streubel, and K. Rudion, "Manual Configuration and Best Setup of Support Vector Machines for Power Quality Classification," in *2021 IEEE Madrid PowerTech, PowerTech 2021 - Conference Proceedings*, Jun. 2021. doi: 10.1109/PowerTech46648.2021.9495006.

[19] O. Mabrouk, L. Hlaoua, and M. N. Omri, "Profile categorization system based on feature reduction," in *International Symposium on Artificial Intelligence and Mathematics, ISAIM 2018*, 2018. Accessed: May 28, 2023. [Online]. Available: https://www.researchgate.net/publication/321244465

[20] Y. Duan, B. Zou, J. Xu, F. Chen, J. Wei, and Y. Y. Tang, "OAA-SVM-MS: A fast and efficient multi-class classification algorithm," *Neurocomputing*, vol. 454, pp. 448–460, Sep. 2021, doi: 10.1016/j.neucom.2021.04.115.

[21] M. M. Manjurul Islam and J. M. Kim, "Reliable multiple combined fault diagnosis of bearings using heterogeneous feature models and multiclass support vector Machines," *Reliab. Eng. Syst. Saf.*, vol. 184, pp. 55–66, Apr. 2019, doi: 10.1016/j.ress.2018.02.012.

[22] I. H. Sarker, "CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks," *Internet of Things (Netherlands)*, vol. 14, p. 100393, Jun. 2021, doi: 10.1016/j.iot.2021.100393.

[23] C. C. Sun, D. J. Sebastian Cardenas, A. Hahn, and C. C. Liu, "Intrusion Detection for Cybersecurity of Smart Meters," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 612–622, 2021, doi: 10.1109/TSG.2020.3010230.

[24] S. Dong, "Multi class SVM algorithm with active learning for network traffic classification," *Expert Syst. Appl.*, vol. 176, no. February, p. 114885, 2021, doi: 10.1016/j.eswa.2021.114885.

[25] Y. Wu, W. W. Lee, Z. Xu, and M. Ni, "Large-scale and robust intrusion detection model combining improved deep belief network with feature-weighted svm," *IEEE Access*, vol. 8, pp. 98600–98611, 2020, doi: 10.1109/ACCESS.2020.2994947.

[26] S. Idris, O. Oyefolahan Ishaq, and N. Ndunagu Juliana, "Intrusion Detection System Based on Support Vector Machine Optimised with Cat Swarm Optimization Algorithm," *2019 2nd Int. Conf. IEEE Niger. Comput. Chapter, Niger. 2019*, Oct. 2019, doi: 10.1109/NIGERIACOMPUTCONF45974.2019.8949676.

[27] K. Thirumala, S. Pal, T. Jain, and A. C. Umarikar, "A classification method for multiple power quality disturbances using EWT based adaptive filtering and multiclass SVM," *Neurocomputing*, vol. 334, pp. 265–274, Mar. 2019, doi: 10.1016/j.neucom.2019.01.038.

[28] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection," *IEEE Access*, vol. 6, no. c, pp. 33789–33795, 2018, doi: 10.1109/ACCESS.2018.2841987.

[29] Y. N. Kunang, S. Nurmaini, D. Stiawan, A. Zarkasi, and F. Jasmir, "Automatic Features Extraction Using Autoencoder in Intrusion Detection System," in *Proceedings of 2018 International Conference on Electrical*

Engineering and Computer Science, ICECOS 2018, Jan. 2019, pp. 219–224. doi: 10.1109/ICECOS.2018.8605181.

[30] M. U. Sapozhnikova, A. V. Nikonov, and A. M. Vulfin, "Intrusion detection system based on data mining technics for industrial networks," in *Proceedings - 2018 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2018*, May 2018. doi: 10.1109/ICIEAM.2018.8728771.

[31] W. A. Safitri, T. Ahmad, and D. P. Hostiadi, "Analyzing Machine Learning-based Feature Selection for Botnet Detection," in *2022 1st International Conference on Information System and Information Technology, ICISIT 2022*, 2022, pp. 386–391. doi: 10.1109/ICISIT54091.2022.9872812.

[32] G. Fahrnberger, "Realtime Risk Monitoring of SSH Brute Force Attacks," in *Communications in Computer and Information Science*, 2022, vol. 1585 CCIS, pp. 75–95. doi: 10.1007/978-3-031-06668-9_8.

[33] L. Nie *et al.*, "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 1, pp. 134–145, Feb. 2022, doi: 10.1109/TCSS.2021.3063538.

[34] R. Sakthiprabha, S. Sivasundarapandian, A. Aranganathan, V. Vedanarayanan, E. Rajinikanth, and T. Gomathi, "Data scientific approach to detect the DoS attack, Probe attack, R2L attack and U2R attack," in *Proceedings of the 2nd IEEE International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2023*, 2023. doi: 10.1109/ACCAI58221.2023.10199636.

[35] R. Wang, H. Jiang, and G. Shi, "A Multi-Layer Hybrid Intrusion Detection Method Based on Nb and SVM," in *Proceedings of 2022 IEEE 4th International Conference on Civil Aviation Safety and Information Technology, ICCASIT 2022*, 2022, pp. 1384–1388. doi: 10.1109/ICCASIT55263.2022.9986813.

[36] S. H. Ahammad *et al.*, "Phishing URL detection using machine learning methods," *Adv. Eng. Softw.*, vol. 173, p. 103288, Nov. 2022, doi: 10.1016/j.advengsoft.2022.103288.

[37] N. V. Sharma and N. S. Yadav, "An optimal intrusion detection system using recursive feature elimination and ensemble of classifiers," *Microprocess. Microsyst.*, vol. 85, p. 104293, Sep. 2021, doi: 10.1016/j.micpro.2021.104293.

[38] R. M. A. Mohammad, "An Enhanced Multiclass Support Vector Machine Model and its Application to Classifying File Systems Affected by a Digital Crime," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 2, pp. 179–190, Feb. 2022, doi: 10.1016/j.jksuci.2019.10.010.

[39] S. Teng, N. Wu, H. Zhu, L. Teng, and W. Zhang, "SVM-DT-based adaptive and collaborative intrusion detection," *IEEE/CAA J. Autom. Sin.*, vol. 5, no. 1, pp. 108–118, Jan. 2018, doi: 10.1109/JAS.2017.7510730.

[40] A. Saber, B. Fergani, and M. Abbas, "Encrypted Traffic Classification: Combining Over-and Under-Sampling through a PCA-SVM," in *Proceedings - PAIS 2018: International Conference on Pattern Analysis and Intelligent Systems*, Dec. 2018. doi: 10.1109/PAIS.2018.8598480.

[41] B. R. Senapati, P. M. Khilar, T. Dash, and R. R. Swain, "AI-assisted Emergency Healthcare using Vehicular Network and Support Vector Machine," *Wirel. Pers. Commun.*, vol. 130, no. 3, pp. 1929–1962, Jun. 2023, doi: 10.1007/S11277-023-10366-8/FIGURES/19.

[42] A. Balasch, M. Beinhofer, and G. Zauner, "The Relative Confusion Matrix, a Tool to Assess Classifiablility in Large Scale Picking Applications," in *Proceedings - IEEE International Conference on Robotics and Automation*, May 2020, pp. 8390–8396. doi: 10.1109/ICRA40945.2020.9197540.

[43] M. Rahbar, S. Amirkhani, A. Chaibakhsh, and F. Rahbar, "Unbalance fault localization in rotating machinery disks using EEMD and optimized multi-class SVM," in *I2MTC 2017 - 2017 IEEE International Instrumentation and Measurement Technology Conference, Proceedings*, Jul. 2017. doi:

10.1109/I2MTC.2017.7969886.

[44] H. Cao, J. Zhang, X. Cao, R. Li, and Y. Wang, "Optimized SVM-Driven Multi-Class Approach by Improved ABC to Estimating Ship Systems State," *IEEE Access*, vol. 8, pp. 206719–206733, 2020, doi: 10.1109/ACCESS.2020.3037251.