

**VISUALISASI POLA SERANGAN *BRUTE FORCE* DENGAN
ALGORITMA *SUPPORT VECTOR MACHINE***

SKRIPSI

**Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana
Komputer**



OLEH :

Friliandi Fathoni

09011381823121

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

HALAMAN PENGESAHAN

VISUALISASI POLA SERANGAN *BRUTE FORCE* DENGAN ALGORITMA *SUPPORT VECTOR MACHINE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar
Sarjana Komputer

Oleh :

Friandi Fathoni

09011381823121

Palembang, ²² Februari 2023

Mengetahui,

Pembimbing 1 Tugas Akhir



Ahmad Heryanto, S. Kom., M.T.
NIP. 198701222015041002

Pembimbing 2 Tugas Akhir



Adi Hermansyah, M.T.
NIK. 1613033004890001

Ketua Jurusan Sistem Komputer



Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 27 Januari 2023

Tim Penguji :

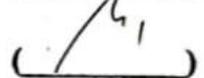
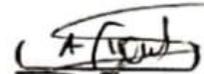
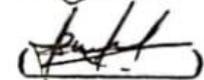
1. **Ketua** : **Kemahyanto Exaudi, M.T.**

2. **Sekretaris** : **Abdurahman, S.Kom., M.Han**

3. **Penguji** : **Sarmayanta Sembiring, M.T.**

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

5. **Pembimbing II** : **Adi Hermansyah, M.T.**



Mengetahui, *n/2/23*

Ketua Jurusan Sistem Komputer



Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda di bawah ini :

Nama : Friiandi Fathoni

NIM : 09011381823121

Judul : Visualisasi Pola Serangan *Brute Force* Dengan Algoritma *Support Vector Machine*

Hasil Pengecekan Software iThenticate/Turnitin : 17%

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

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Palembang, 22 Februari 2023



Friiandi Fathoni
NIM. 09011381823121

KATA PENGANTAR

Puji serta syukur kita panjatkan kehadirat Tuhan Yang Maha Esa juga maha pengasih dan penyayang atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini yang berjudul **“Visualisasi pola serangan *Brute Force* dengan Algoritma *Support Vector Machine*”**.

Isi dari Tugas Akhir ini sendiri menjelaskan tentang tahapan dalam visualisasi pola serangan yang ada pada *Brute Force* menggunakan algoritma *Support Vector Machine*, yang sebelumnya data pada *Brute Force* diambil dari dataset. Penulis berharap agar hasil karya tulis ini dapat bermanfaat untuk orang banyak, baik untuk penulis sendiri ataupun peneliti lainnya yang tertarik untuk meneliti tentang visualisasi pola serangan *Brute Force*.

Pada kesempatan ini penulis mengucapkan terima kasih kepada beberapa pihak yang telah membantu atas saran dan dukungan dalam menyelesaikan Tugas Akhir. Oleh karena itu, penulis ingin mengucapkan rasa syukur dan terima kasih sebesar besarnya kepada :

1. Tuhan Yang Maha Esa, atas hikmat dan rahmat-Nya yang telah diberikan kepada saya, sehingga dapat menyelesaikan Tugas Akhir dalam keadaan sehat, baik dan lancar.
2. Kedua orang tua saya yang telah membesarkan saya penuh kasih sayang serta telah memberikan dukungan yang sangat besar beserta doa yang terbaik untuk saya selama ini.
3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

4. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Huda Ubaya, M.T., selaku Dosen Pembimbing akademik.
6. Bapak Ahmad Heryanto, S.Kom, M.T., selaku Dosen Pembimbing 1 Tugas Akhir dan Bapak Adi Hermansyah, M.T., selaku Dosen Pembimbing 2 Tugas Akhir yang telah berkenan menjadi pembimbing dan memberikan banyak ilmu yang bermanfaat kepada saya.
7. Teman – teman saya di Jurusan Sistem Komputer, terkhusus teman-teman Laboratorium di Laboratorium Jaringan Komputer.
8. Dan semua pihak yang telah membantu.

Penulis menyadari bahwa banyak kekurangan di dalam Tugas Akhir ini sehingga jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangat diperlukan dalam rangka penyegeraan perbaikan Tugas Akhir sebagai bahan serta ide baru untuk pembahasan penelitian yang berkaitan.

Palembang, 22 Februari 2023

Penulis,



Friiandi Fathoni
NIM. 09011381823121

VISUALIZATION OF BRUTE FORCE ATTACK PATTERNS WITH SUPPORT VECTOR MACHINE ALGORITHM

Friandi Fathoni (09011381823121)

Computer Engineering Department, Computer Science Faculty, Sriwijaya
University

Email : friliandifathoni22@gmail.com

ABSTRACT

Brute force is one of many attacks that are often used by hackers in carrying out the cyber crimes. For recognizing the attack patterns visualization is carried out, so that in presenting this research, looking for attack patterns using parallel coordinates and support vector machines as the classification. In this study, the SVM classification uses several kernels which later will be compared with the highest average values, namely, radial basis function kernels, linear kernels, polynomial kernels, and sigmoid kernels. In the classification using the Support Vector Machine (SVM) method to determine accuracy, precision, recall and F1-score using the confusion matrix technique. In this study using the CIC-IDS2017 dataset, after the research was carried out the Radial Basis Function kernel became the kernel with the best average value.

Keywords : Brute Force, Machine Learning, Support Vector Machine, SVM kernels.

Palembang, ²²February 2023

Supervisor



Ahmad Heryanto, S.Kom, M.T.
NIP. 198701222015041002

Co-Supervisor



Adi Hermansyah, M.T.
NIK. 1613033004890001



Acknowledged

Head of Computer Systems Departement



Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

VISUALISASI POLA SERANGAN *BRUTE FORCE* DENGAN ALGORITMA *SUPPORT VECTOR MACHINE*

Friandi Fathoni (09011381823121)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : friandifathoni22@gmail.com

ABSTRAK

Brute force adalah salah satu dari banyaknya serangan yang sering digunakan oleh para peretas dalam melakukan aksi kejahatan *cyber*. Adapun untuk mengetahui pola serangan tersebut dilakukanlah visualisasi, sehingga dalam penyajian penelitian ini mencari pola serangan dengan menggunakan paralel koordinat dan *support vector machine* sebagai pengklasifikasiannya. Pada penelitian ini, klasifikasi SVM menggunakan beberapa kernel yang nantinya akan dibandingkan nilai rata-rata tertingginya yaitu, kernel *radial basis function*, kernel *linear*, kernel *polynomial*, dan kernel *sigmoid*. Pada klasifikasi menggunakan metode *Support Vector Machine* (SVM) untuk mengetahui akurasi, presisi, *recall* dan *F1-score* menggunakan teknik *confusion matrix*. Pada penelitian ini menggunakan dataset CIC-IDS2017, setelah penelitian dilakukan kernel *Radial Basis Function* menjadi kernel dengan nilai rata-rata terbaik.

Kata Kunci : *Brute Force*, *Machine Learning*, *Support Vector Machine*, Kernel SVM.

Palembang, ^v Februari 2023

Pembimbing 1 Tugas Akhir



Ahmad Hervanto S.Kom, M.T.
NIP. 198701222015041002

Pembimbing 2 Tugas Akhir



Adi Hermansyah, M.T.
NIK. 1613033004890001

Mengetahui,
Ketua Jurusan Sistem Komputer



Dr. H. Sukemi, M.T.
NIP. 196612032006041001

DAFTAR ISI

HALAMAN PENGESAHAN.....	Error! Bookmark not defined.
LEMBAR PERSETUJUAN.....	Error! Bookmark not defined.
HALAMAN PERNYATAAN.....	Error! Bookmark not defined.
KATA PENGANTAR.....	iv
ABSTRACT.....	Error! Bookmark not defined.
ABSTRAK.....	Error! Bookmark not defined.
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Tujuan.....	3
1.3 Manfaat.....	4
1.4 Perumusan Masalah.....	4
1.5 Batasan Masalah.....	4
1.6 Metodologi Penelitian.....	5
1.7 Sistematika Penelitian.....	6
BAB II TINJAUAN PUSTAKA.....	7
2.1 Penelitian Terdahulu.....	7
2.2 Ringkasan Hasil Kajian Literatur.....	21
2.3 Visualisasi Pola Serangan.....	27
2.3.1 Manfaat Visualisasi.....	28
2.4 Serangan Brute Force.....	29
2.4.1 Metode Serangan <i>Brute Force</i> Secara Umum.....	30
2.4.2 Karakteristik Serangan Brute Force.....	32
2.5 <i>Artificial Intelligence</i>	33
2.6 Machine Learning.....	34
2.7 <i>Support Vector Machine</i>	36
2.7.1 <i>Support Vector Machine Hyperplane</i>	37
2.7.2 <i>Support Vector Machine Kernels</i>	37
2.7.3 Keuntungan Penggunaan Metode <i>Support Vector Machine</i>	39
2.8 <i>Jupyter Notebook</i>	39
2.9 Confusion Matrix.....	40

BAB III METODOLOGI PENELITIAN	42
3.1 Pendahuluan.....	42
3.2 Persiapan Dataset.....	42
3.3 Lingkungan <i>Hardware</i> dan <i>Software</i>	42
3.3.1 Perangkat Keras (Hardware)	42
3.3.2 Perangkat Lunak (Software).....	43
3.4 Kerangka Kerja Penelitian	45
3.5 <i>Algoritma Support Vector Machine</i>	47
3.6 Skenario Penelitian	49
3.7 Pseudocode Support Vector Machine	50
3.8 Preprocessing.....	51
3.9 Visualisasi	52
BAB IV HASIL DAN ANALISA.....	53
4.1 Pengolahan Dataset.....	53
4.2 Random Forest Classifier	56
4.3 Visualisasi Pola dan Klasifikasi Kernel SVM.....	57
4.3.1 Hasil Klasifikasi dan Confusion Matrix Dari Radial Basis Function Kernel	58
4.3.2 Hasil Klasifikasi dan Confusion Matrix Dari Linear Kernel.....	61
4.3.3 Hasil Klasifikasi dan Confusion Matrix Dari Polynomial Kernel	64
4.3.4 Hasil Klasifikasi dan Confusion Matrix Dari Sigmoid Kernel	67
4.4 Perbandingan Hasil	70
BAB V KESIMPULAN DAN SARAN.....	71
5.1 Kesimpulan.....	71
5.2 Saran	71
DAFTAR PUSTAKA.....	72
LAMPIRAN.....	78

DAFTAR GAMBAR

Gambar 2. 1 Tahapan Visualisasi	28
Gambar 2. 2 Serangan Brute Force pada Service SSH.....	30
Gambar 2. 3 Support Vector Machine Hyperplane	37
Gambar 3. 1 Kerangka Kerja Penelitian	45
Gambar 3. 2 Flowchart Support Vector Machine	47
Gambar 3. 3 Skenario Penelitian	49
Gambar 4. 1 Jumlah Kolom Dataset.....	53
Gambar 4. 2 Visualisasi Perbandingan Jumlah Data.....	55
Gambar 4. 3 Visualisasi Perbandingan Data setelah Pemotongan Data.....	55
Gambar 4. 4 Skor Hasil Random Forest Classifier	56
Gambar 4. 5 Hasil Visualisasi dari 3 Fitur Variabel.....	57
Gambar 4. 6 Hasil Akurasi Rbf Kernel	58
Gambar 4. 7 Confusion Matrix.....	59
Gambar 4. 8 ROC Curve	60
Gambar 4. 9 Hasil Akurasi Linear Kernel.....	61
Gambar 4. 10 Confusion Matrix.....	61
Gambar 4. 11 ROC Curve	63
Gambar 4. 12 Hasil Akurasi Polynomial Kernel.....	64
Gambar 4. 13 Confusion Matrix.....	64
Gambar 4. 14 ROC Curve	66
Gambar 4. 15 Hasil Akurasi Sigmoid Kernel.....	67
Gambar 4. 16 Confusion Matrix.....	67
Gambar 4. 17 ROC Curve	69

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu.....	7
Tabel 2. 2 Pebandingan antara kunci dan permutasi	32
Tabel 2. 3 Nilai yang dihasilkan confusion matrix	40
Tabel 3. 1 Spesifikasi Perangkat Keras Komputer yang Digunakan.....	43
Tabel 3. 2 Spesifikasi Perangkat Lunak yang Digunakan.....	43
Tabel 4. 1 Tampilan Lengkap Fitur Variabel Dalam Kolom	53
Tabel 4. 2 Fitur yang Dipilih	57
Tabel 4. 3 Tabel Perbandingan Hasil	70

BAB I

PENDAHULUAN

1.1 Latar Belakang

Serangan *brute force* adalah jenis serangan yang berupaya mengakses sebuah sistem ataupun jaringan dengan menebak-nebak kata sandi pengguna secara paksa [1]. Teknik brute force attack banyak digunakan untuk crack password atau kata sandi. Serangan brute force biasanya terjadi pada server yang menyediakan layanan seperti WEB, DNS, FTP, MAIL, dan SSH, kemudian layanan protokol yang diserang adalah SSH dan TELNET [2].

Dalam proses visualisasi dan machine learning, serangan brute force dapat divisualisasikan secara grafis. Visualisasi ini merupakan aspek yang vital karena akan mempermudah melihat akurasi serta pola anomaly serangan *brute force* yang biasanya terjadi pada server yang menyediakan beberapa layanan maupun layanan protocol. Dalam konteks ini, pola serangan atau juga anomaly yang bentuknya akan terlihat menjadi grafik-grafik dalam *machine learning* yang digunakan.

Visualisasi data sangat penting dalam menganalisis sebuah data secara ringkas dan juga memberikan kemampuan untuk mengeksplorasi data tersebut [3]. Pada teknik visualisasi untuk analisis keamanan jaringan, menjelaskan visualisasi jaringan memungkinkan analisis keamanan dengan cepat mengidentifikasi pola yang mencurigakan.

Pada penelitian sebelumnya [4], dengan judul “*Detection of SSH Brute Force Attacks Using Aggregated Netflow Data*”, membahas tentang beberapa metode untuk mendeteksi serangan *brute force* pada SSH yang telah didistribusikan, metode yang digunakan adalah *K-Nearest Neighbor*, *Decision Trees*, dan *Naïve Bayes*. Hasil dari penelitian ini adalah dimana dapat mengidentifikasi serangan untuk menentukan apakah telah terjadi serangan atau juga belum terjadinya serangan. Kekurangan pada penelitian ini adalah belum adanya perbandingan antara kinerja fitur agregat dan fitur netflow untuk deteksi serangan *brute force*.

Dalam penelitian sebelumnya [5], dengan judul “*Clustering of SSH brute-force attack logs using k-clique percolation*”, membahas penggunaan metode *k-Clique Percolation*, untuk mengelompokkan log serangan *brute force* pada layanan SSH. Hasil dari penelitian ini didapat percobaan $k = 3$ dan $k = 4$ dimana I diatur dari 0,1 sampai 0,5. Nilai k yang lebih rendah akan menghasilkan cluster yang tidak signifikan sementara nilai yang lebih tinggi mendorong enumerasi perkolasi *k-clique* yang sangat lambat. Oleh karena itu, pemilihan $k = 3$ dan $I = 0,3$ atau $0,4$ karena memberikan hasil pengelompokan terbaik setelah inspeksi manual. Kekurangan pada penelitian ini adalah kurang optimalnya metode yang digunakan dalam pengelompokkan serangan *brute force* SSH.

Pada penelitian yang dilakukan oleh [6], yang berjudul “*Machine Learning for Detecting Brute Force Attacks at The Network Level*”, menggunakan data netflow digabungkan dengan pendekatan *machine learning* untuk mendeteksi serangan *brute force ssh* pada level jaringan. Penelitian ini menggunakan *machine learning* yang penggunaannya secara otomatis, tidak seperti metode *signature* yang masih mengekstrak pola secara manual. Hasil dari penelitian ini adalah akurasi dari metode *machine learning* dalam hal ini

menggunakan *naïve bayes* adalah 99%. Kelemahan dari penelitian ini adalah masih terabaikannya fitur-fitur bagus saat membangun sebuah model.

Dalam penelitian sebelumnya [7] , yang berjudul “*SSH-Brute Force Attack Detection Model Based on Deep Learning*”, membahas tentang mekanisme yang efisien untuk deteksi serangan *brute force ssh* berdasarkan algoritma *machine learning*, yang digunakan di penelitian ini yaitu *convolutional neural network*. Hasil dari penelitian ini adalah akurasi epoch yang didapat sebesar 94 %, kemudian akurasi klasifikasi sebesar 94.3 % dan tingkat presisi 92.5 %, F1 sebesar 91.8 % dan juga *recall rate* sebesar 97.8 %. Kelemahan dari penelitian ini adalah belum banyaknya akan penggunaan *deep learning* sehingga belum banyaknya untuk perbandingan penelitian.

Pada penelitian lainnya juga [8] , yang berjudul “*Real Time Detection and Classification of DDoS Attacks Using Enhanced SVM with String Kernels*”, membahas tentang deteksi *real-time* dan klasifikasi serangan DDOS menggunakan metode Enhanced SVM dengan *String Kernels*. Penelitian tersebut membuat sistem deteksi anomali yang dirancang menggunakan metode Enhanced SVM dengan kernel string untuk mendeteksi serangan DDos *Real-Time*. Atribut perilaku yang digunakan ialah akses pengguna normal sebagai sampel pelatihan untuk ESVM yang menghasilkan file model (pola). Kemudian data normal dan serangan dikumpulkan untuk digunakan sebagai sampel uji ESVM. Hasil dari penelitian ini didapat akurasi dari klasifikasi sebesar 99 %. Kelemahan penelitian ini adalah belum baiknya hasil klasifikasi dari beberapa kernel yang digunakan.

Dari berbagai referensi diatas dan beberapa rujukan sebelumnya, maka pada penelitian tugas akhir ini, akan memvisualisasikan pola serangan *brute force* menggunakan metode atau algoritma *support vector machine* digunakan untuk memvisualisasi serangan *brute force*.

1.2 Tujuan

Tujuan dari penulisan tugas akhir ini, yaitu :

1. Mengenali pola serangan *Brute force*.

2. Menerapkan algoritma *Support vector machine* untuk visualisasi serangan *Brute force*.
3. Menampilkan akurasi dan mencari nilai terbaik dari kernel *Support Vector Machine*.

1.3 Manfaat

Manfaat dari penulisan tugas akhir ini, yaitu :

1. Dapat memvisualisasikan serangan *Brute force*.
2. Dapat memberi kemudahan dalam mengenali serangan *Brute force*.
3. Dapat menampilkan akurasi dan mencari nilai terbaik dari kernel *Support Vector Machine*.

1.4 Perumusan Masalah

Ada beberapa masalah yang timbul dari latar belakang yang telah dibuat sebelumnya yaitu, visualisasi dan klasifikasi terhadap brute force cenderung menggunakan metode *machine learning* yang masih terbatas, serta teknik tersebut kurang mempertimbangkan fitur yang terkait didalam serangan mengakibatkan dampak negatif pada akurasi yang didapat. Lalu tidak semua Teknik yang digunakan sepenuhnya menggunakan visualisasi dalam serangan *brute force*. Solusi untuk permasalahan tersebut adalah dengan pengoptimalan visualisasi sehingga didapat akurasi yang baik dan pola traffic serangan yang jelas. Kemudian bagaimana memvisualisasikan serangan brute force ini kedalam bentuk grafik yang mudah dimengerti sehingga dapat dilihat bagaimana pola serangan tersebut, solusinya adalah dengan memilih fitur yang tepat dalam visualisasi dalam hal ini *support vector machine*.

1.5 Batasan Masalah

Adapun batasan masalah dari tugas akhir ini, yaitu :

1. Tidak melakukan pendeteksian terhadap serangan *Brute Force*.

2. Visualisasi serangan *brute force* tidak diujicoba pada lalu lintas jaringan *real time*.
3. Tidak membahas bagaimana pencegahan serangan *brute force*.
4. Tidak diuji pada trafik jaringan terenkripsi.

1.6 Metodologi Penelitian

Tugas akhir ini menggunakan metodologi sebagai berikut :

1. Metode Studi Pustaka dan Literature

Metode pengumpulan informasi tentang penelitian yang akan dilakukan menjadi dasar studi literatur. Untuk mendukung metodologi dan pendekatan penelitian, referensi ini bersumber dari jurnal, buku, internet, dan sumber lainnya.

2. Metode Pembuatan Model

Pada metode ini membuat suatu perancangan pemodelan dengan menggunakan diagram flowchart.

3. Metode Pengujian

Untuk mendapatkan hasil pengujian yang sesuai dengan batasan masalah dan parameter yang telah ditentukan maka akan dilakukan pengujian pada bagian ini berdasarkan penelitian sebelumnya.

4. Metode Analisis

Setelah tahap pengujian akan dilakukan analisis berdasarkan identifikasi masalah. Tujuannya adalah memperoleh data objektif dari analisis hasil pengolahan data serta dapat dilakukannya pengembangan pada penelitian sebelumnya.

5. Metode Kesimpulan

Penarikan kesimpulan dari studi pustaka, metodologi, dan analisa hasil pengujian.

1.7 Sistematika Penelitian

Sebuah sistematika penelitian dikembangkan untuk proyek akhir ini untuk memudahkan proses penyusunan dan memperjelas isi dari setiap bab:

BAB I. PENDAHULUAN

Latar Belakang, Tujuan, Manfaat, Rumusan Masalah, Batasan Masalah, Metodologi Penelitian, dan Sistematika Penulisan merupakan pokok bahasan penelitian yang dibahas dalam bab ini.

BAB II. TINJAUAN PUSTAKA

Landasan teori untuk penelitian tugas akhir tentang Visualisasi, Brute Force, dan Support Vector Machines diberikan dalam bab ini, beserta informasi tentang penelitian terkait.

BAB III. METODOLOGI PENELITIAN

Bab ini berisi deskripsi sistematis tentang proses di mana penelitian ini dilakukan. Akan menjelaskan tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV. PENGUJIAN DAN ANALIS

Hasil pengujian disajikan dalam bab ini, disertai dengan analisis setiap kumpulan data berdasarkan parameter yang telah ditetapkan sebelumnya.

BAB V. KESIMPULAN DAN SARAN

Kesimpulan tentang temuan penelitian, yang diharapkan sejalan dengan BAB I, dan rekomendasi untuk penelitian mendatang disertakan dalam bab ini.

DAFTAR PUSTAKA

- [1] J. Luxemburk, K. Hynek, and T. Cejka, "Detection of HTTPS Brute-Force Attacks with Packet-Level Feature Set," *2021 IEEE 11th Annu. Comput. Commun. Work. Conf. CCWC 2021*, pp. 114–122, 2021, doi: 10.1109/CCWC51732.2021.9375998.
- [2] Y. Wu, P. M. Cao, A. Withers, Z. T. Kalbarczyk, and R. K. Iyer, "Mining Threat Intelligence from Billion-scale SSH Brute-Force Attacks," no. February, 2021, doi: 10.14722/diss.2020.23007.
- [3] T. Munz, D. V ath, P. Kuznecov, N. T. Vu, and D. Weiskopf, "Visualization-based improvement of neural machine translation," *Comput. Graph.*, vol. 103, pp. 45–60, 2022, doi: 10.1016/j.cag.2021.12.003.
- [4] M. M. Najafabadi, T. M. Khoshgoftaar, C. Calvert, and C. Kemp, "Detection of SSH brute force attacks using aggregated netflow data," *Proc. - 2015 IEEE 14th Int. Conf. Mach. Learn. Appl. ICMLA 2015*, pp. 283–288, 2016, doi: 10.1109/ICMLA.2015.20.
- [5] H. Studiawan, B. A. Pratomo, and R. Anggoro, "Clustering of SSH brute-force attack logs using k-clique percolation," *Proc. 2016 Int. Conf. Inf. Commun. Technol. Syst. ICTS 2016*, pp. 39–42, 2017, doi: 10.1109/ICTS.2016.7910269.
- [6] M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya, and R. Zuech, "Machine learning for detecting brute force attacks at the network level," *Proc. - IEEE 14th Int. Conf. Bioinforma. Bioeng. BIBE 2014*, pp. 379–385, 2014, doi: 10.1109/BIBE.2014.73.
- [7] S. Kahara Wanjau, G. M. Wambugu, and G. Ndung'u Kamau, "SSH-Brute Force Attack Detection Model based on Deep Learning," *Int. J. Comput. Appl. Technol. Res.*, vol. 10, no. 01, pp. 42–50, 2021, [Online]. Available: www.ijcat.com.

- [8] A. Ramamoorthi, T. Subbulakshmi, and S. M. Shalinie, "Real time detection and classification of DDoS attacks using enhanced SVM with string kernels," *Int. Conf. Recent Trends Inf. Technol. ICRTIT 2011*, pp. 91–96, 2011, doi: 10.1109/ICRTIT.2011.5972281.
- [9] D. Stiawan, S. Sandra, E. Alzahrani, and R. Budiarto, "Comparative analysis of K-Means method and Naïve Bayes method for brute force attack visualization," *2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017*, pp. 177–182, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905286.
- [10] F. Akhbardeh, F. Vasefi, N. MacKinnon, M. Amini, A. Akhbardeh, and K. Tavakolian, "Classification and Assessment of Hand Arthritis Stage using Support Vector Machine," *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS*, pp. 4080–4083, 2019, doi: 10.1109/EMBC.2019.8857022.
- [11] E. U. Haq, J. Huang, H. Xu, K. Li, and F. Ahmad, "A hybrid approach based on deep learning and support vector machine for the detection of electricity theft in power grids," *Energy Reports*, vol. 7, pp. 349–356, 2021, doi: 10.1016/j.egyr.2021.08.038.
- [12] J. A. Perez-Diaz, I. A. Valdovinos, K. K. R. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.
- [13] S. Kar, B. Tudu, and R. Bandyopadhyay, "Identification and Classification of Sudan Dye i Adulterants in Turmeric Powder by Nir Spectroscopy and Support Vector Machine," *ISOEN 2019 - 18th Int. Symp. Olfaction Electron. Nose, Proc.*, pp. 1–4, 2019, doi: 10.1109/ISOEN.2019.8823529.
- [14] S. Shahbudin, M. Zamri, M. Kassim, S. A. C. Abdullah, and S. I. Suliman, "Weed classification using one class support vector machine," *2017 Int. Conf. Electr. Electron. Syst. Eng. ICEESE 2017*, vol. 2018-Janua, pp. 7–10, 2018, doi: 10.1109/ICEESE.2017.8298404.
- [15] L. Mohan, J. Pant, P. Suyal, and A. Kumar, "Support Vector Machine Accuracy Improvement with Classification," *Proc. - 2020 12th Int. Conf.*

- Comput. Intell. Commun. Networks, CICN 2020*, pp. 477–481, 2020, doi: 10.1109/CICN49253.2020.9242572.
- [16] F. Borges *et al.*, “An Unsupervised Method based on Support Vector Machines and Higher-Order Statistics for Mechanical Faults Detection,” *IEEE Lat. Am. Trans.*, vol. 18, no. 6, pp. 1093–1101, 2020, doi: 10.1109/TLA.2020.9099687.
- [17] G. Cheng and X. Tong, “Fuzzy clustering multiple kernel support vector machine,” *Int. Conf. Wavelet Anal. Pattern Recognit.*, vol. 2018-July, pp. 7–12, 2018, doi: 10.1109/ICWAPR.2018.8521307.
- [18] S. Y. Yerima and S. Sezer, “DroidFusion: A Novel Multilevel Classifier Fusion Approach for Android Malware Detection,” *IEEE Trans. Cybern.*, vol. 49, no. 2, pp. 453–466, 2019, doi: 10.1109/TCYB.2017.2777960Y.
- [19] R. Taheri, M. Ghahramani, R. Javidan, M. Shojafar, Z. Pooranian, and M. Conti, “Similarity-based Android malware detection using Hamming distance of static binary features,” *Futur. Gener. Comput. Syst.*, vol. 105, pp. 230–247, 2020, doi: 10.1016/j.future.2019.11.034.
- [20] A. M. Ahmed, S. H. Ahmed, and O. H. Ahmed, “Enhancing 3D-playfair algorithm to support all the existing characters and increase the resistanceto brute force and frequency analysis attacks,” *Int. Conf. Curr. Res. Comput. Sci. Inf. Technol. ICCIT 2017*, pp. 81–85, 2017, doi: 10.1109/CRCSIT.2017.7965538.
- [21] P. D. Windha Mega and Haryoko, “Optimization of parameter support vector machine (SVM) using genetic algorithm to review go-jek’s services,” *2019 4th Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2019*, vol. 6, pp. 301–304, 2019, doi: 10.1109/ICITISEE48480.2019.9003894.
- [22] R. Kozik, “Distributing extreme learning machines with Apache Spark for NetFlow-based malware activity detection,” *Pattern Recognit. Lett.*, vol. 101, pp. 14–20, 2018, doi: 10.1016/j.patrec.2017.11.004.

- [23] A. Nursetyo, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto, and C. A. Sari, "Website and Network Security Techniques against Brute Force Attacks using Honeypot," *Proc. 2019 4th Int. Conf. Informatics Comput. ICIC 2019*, 2019, doi: 10.1109/ICIC47613.2019.8985686.
- [24] Laatansa, R. Saputra, and B. Noranita, "Analysis of GPGPU-Based Brute-Force and Dictionary Attack on SHA-1 Password Hash," *ICICOS 2019 - 3rd Int. Conf. Informatics Comput. Sci. Accel. Informatics Comput. Res. Smarter Soc. Era Ind. 4.0, Proc.*, pp. 1–4, 2019, doi: 10.1109/ICICoS48119.2019.8982390.
- [25] Y. Xin *et al.*, "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, no. c, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.
- [26] M. Nadeem, A. Arshad, S. Riaz, S. S. Band, and A. Mosavi, "Intercept the cloud network from brute force and ddos attacks via intrusion detection and prevention system," *IEEE Access*, vol. 9, pp. 152300–152309, 2021, doi: 10.1109/ACCESS.2021.3126535.
- [27] P. K. Illa, B. Parvathala, and A. K. Sharma, "Stock price prediction methodology using random forest algorithm and support vector machine," *Mater. Today Proc.*, no. xxxx, 2021, doi: 10.1016/j.matpr.2021.10.460.
- [28] J. Park, J. Kim, B. B. Gupta, and N. Park, "Network Log-Based SSH Brute-Force Attack Detection Model," *Comput. Mater. Contin.*, vol. 68, no. 1, pp. 887–901, 2021, doi: 10.32604/cmc.2021.015172.
- [29] F. Camastra, V. Capone, A. Ciaramella, A. Riccio, and A. Staiano, "Prediction of environmental missing data time series by Support Vector Machine Regression and Correlation Dimension estimation," *Environ. Model. Softw.*, vol. 150, no. April 2021, p. 105343, 2022, doi: 10.1016/j.envsoft.2022.105343.
- [30] S. Saito, K. Maruhashi, M. Takenaka, and S. Torii, "TOPASE: Detection and prevention of brute force attacks with disciplined IPs from IDS logs," *J. Inf. Process.*, vol. 24, no. 2, pp. 217–226, 2016, doi:

10.2197/ipsjjip.24.217.

- [31] A. Patil, A. Laturkar, S. V. Athawale, R. Takale, and P. Tathawade, "A multilevel system to mitigate DDOS, brute force and SQL injection attack for cloud security," *IEEE Int. Conf. Information, Commun. Instrum. Control. ICICIC 2017*, vol. 2018-Janua, pp. 1–7, 2018, doi: 10.1109/ICOMICON.2017.8279028.
- [32] A. V. Pawar and A. R. Dani, "Privacy preserving framework for brute force attacks in cloud environment," *Int. J. High Perform. Comput. Netw.*, vol. 10, no. 1–2, pp. 91–99, 2017, doi: 10.1504/IJHPCN.2017.083205.
- [33] H. Khaled, "Enhancing recursive brute force algorithm with static memory allocation: Solving motif finding problem as a case study," *Proc. - ICCES 2019 2019 14th Int. Conf. Comput. Eng. Syst.*, pp. 66–70, 2019, doi: 10.1109/ICCES48960.2019.9068158.
- [34] R. Pretorius and B. J. Kotze, "An Artificial Intelligence Energy Management System for An Educational Building," *2021 South. African Univ. Power Eng. Conf. Mechatronics/Pattern Recognit. Assoc. South Africa, SAUPEC/RobMech/PRASA 2021*, 2021, doi: 10.1109/SAUPEC/RobMech/PRASA52254.2021.9377027.
- [35] H. Elaidi, Y. Elhaddar, Z. Benabbou, and H. Abbar, "An idea of a clustering algorithm using support vector machines based on binary decision tree," *2018 Int. Conf. Intell. Syst. Comput. Vision, ISCV 2018*, vol. 2018-May, no. 5, pp. 1–5, 2018, doi: 10.1109/ISACV.2018.8354024.
- [36] S. Tong, C. Yanqiao, and Z. Yuan, "Fault prediction of marine diesel engine based on time series and support vector machine," *Proc. - 2020 Int. Conf. Intell. Des. ICID 2020*, no. Icid, pp. 75–81, 2020, doi: 10.1109/ICID52250.2020.00023.
- [37] G. A. Pethunachiyar, "Classification of diabetes patients using kernel based support vector machines," *2020 Int. Conf. Comput. Commun. Informatics, ICCCI 2020*, pp. 22–25, 2020, doi: 10.1109/ICCCI48352.2020.9104185.

- [38] A. Patle and D. S. Chouhan, "SVM kernel functions for classification," *2013 Int. Conf. Adv. Technol. Eng. ICATE 2013*, 2013, doi: 10.1109/ICAdTE.2013.6524743.
- [39] A. P. Koenzen, N. A. Ernst, and M. A. D. Storey, "Code Duplication and Reuse in Jupyter Notebooks," *Proc. IEEE Symp. Vis. Lang. Human-Centric Comput. VL/HCC*, vol. 2020-Augus, 2020, doi: 10.1109/VL/HCC50065.2020.9127202.
- [40] Y. Xiong, "Building text hierarchical structure by using confusion matrix," *2012 5th Int. Conf. Biomed. Eng. Informatics, BMEI 2012*, no. Bmei, pp. 1250–1254, 2012, doi: 10.1109/BMEI.2012.6513202.