VISUALISASI POLA SERANGAN *BRUTE FORCE* MENGGUNAKAN METODE K – NEAREST NEIGHBOR

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

DISUSUN OLEH :

Muhammad Robby Bahari

09011381823099

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

HALAMAN PENGESAHAN

VISUALISASI POLA SERANGAN *BRUTE FORCE* MENGGUNAKAN METODE K – NEAREST NEIGHBOR

TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

Oleh :

Muhammad Robby Bahari
09011381823099

Palembang, 27 Juni 2022

Mengetahui,

Pembimbing 1 Tugas Akhir	Pembimbing 2 Tugas Akhir
Ahmad Heryanto, S. Kom, M.T.	**Adi Hermansyah, M.T.**
NIP. 198701222015041002	**NIK. 1613033004890001**

Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 16 Juni 2022

Tim Penguji :

1. **Ketua** : **Huda Ubaya, M.T.**
2. **Sekretaris** : **Aditya Putra P Prasetyo, S.Kom., M.T.**
3. **Pembimbing I** : **Ahmad Heryanto, S.Kom., M.T.**
4. **Pembimbing II** : **Adi Hermansyah, M.T.**
5. **Penguji** : **Deris Stiawan, M.T., Ph.D.**

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : **Muhammad Robby Bahari**

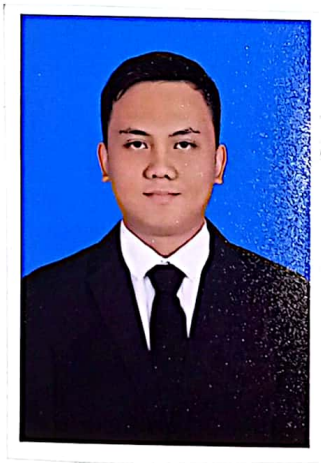
NIM : **09011381823099**

Judul : **Visualisasi Pola Serangan *Brute Force* Menggunakan Metode K-Nearest Neighbor**

Hasil Pengecekan Software iTenticate/Turnitin : 6%

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

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



Palembang, 27 Juni 2022

Muhammad Robby Bahari

NIM. 09011381823099

HALAMAN PERSEMBAHAN

"Perjalanan hidup tidaklah mudah, dan hidup tidak akan menjadi mudah. Banyak rintangan dan cobaan yang harus dilalui dalam kehidupan ini. Tetapi dengan semangat yang tinggi dan diiringi dengan doa serta bersifat optimis dalam segala situasi, maka rintangan dan cobaan tersebut hanyalah seperti badai yang akan berlalu."

(Penulis, Muhammad Robby Bahari)

Skripsi ini kupersembahkan untuk :

Kedua Orang Tuaku.
(Juli Firdaus dan Rosita)

Keluarga Besarku.
(Daniel Lunda dan Suwitak)

Teman – temanku.
(Sistem Komputer 2018)

Dan Almamaterku.
(Universitas Sriwijaya)

"Pendidikan adalah senjata paling mematikan di dunia, karena dengan pendidikan, kamu dapat mengubah dunia."
(Nelson Mandela)

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيْم

Assalamu'alaikum Warahmatullahi Wabarakatuh

Marilah kita panjatkan puji serta syukur atas kehadirat Allah SWT karena atas berkat hidayah dan karunia – Nya penulis telah dapat menyelesaikan penyusunan tugas akhir ini yang berjudul "**Visualisasi Pola Serangan *Brute Force* Menggunakan Metode K – Nearest Neighbor**". Sebelumnya, penulis ingin memberikan serta mengucapkan terima kasih kepada beberapa pihak yang senantiasa memberikan ide, masukan, kritik, serta motivasi selama penulis melakukan penyusunan Tugas Akhir. Ucapan terima kasih tersebut ingin penulis sampaikan kepada :

1. Allah SWT yang senantiasa telah memberikan rahmat serta karunia – Nya sehingga penulis bisa menyelesaikan penulisan Tugas Akhir ini.
2. Orang tua saya tercinta Juli Firdaus dan Rosita yang tidak letih - letih dalam mengasuh serta mendidik saya hingga saat ini dan tak ada hentinya juga dalam memberikan nasihat, semangat, serta juga dalam memberikan motivasi.
3. Bapak Jaidan Jauhari, S. Pd. M.T. yang merupakan Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T., yang merupakan Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing 1 dan Bapak Adi Hermansyah, M.T. selaku Dosen Pembimbing 2 Tugas Akhir yang telah berkenan meluangkan waktu dan tenaga dalam membimbing, memberikan saran serta motivasi kepada penulis selama proses penulisan Tugas Akhir ini.
6. Bapak Dr. Firdaus, M.Kom. selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer penulis saat ini.

7. Paman saya Joni Hidayat yang telah memberikan berbagai bantuan selama penulis menjalani masa perkuliahan hingga akhir.
8. Mbak Sari Nuzulastri dan Mbak Renny Virgasari selaku admin jurusan sistem komputer yang telah berjasa dalam membantu permasalahan administrasi penulis.
9. Teman saya Muhammad Wahyu Fadli, Muhammad Daffa Badran Thoriq, dan juga Gulfi Oktariani yang pernah membantu penulis dalam masa – masa sulit saat pengerjaan tugas akhir.
10. Rizky Angga Pratama dan M. Alfat Hayatur Rizon selaku asisten lab jaringan komputer kampus bukit yang telah meminjamkan fasilitas lab semasa pengerjaan tugas akhir.
11. Ajie Salahudin Prima, A Josman Pratama, dan juga Ronnie Radhitya Raffi yang merupakan teman terdekat penulis yang selalu menghibur dalam masa – masa sulit perkuliahan.
12. Teman – teman saya lainnya yang selalu menghibur, menemani dan juga memberikan motivasi kepada penulis selama dalam masa perkuliahan.
13. Semua pihak yang terlibat yang telah turut ikut membantu, baik itu dalam memberikan masukan dan ide, kritik, maupun juga memberikan semangat kepada penulis yang mana tidak bisa disebutkan satu persatu.

Penulis menyadari bahwasanya penyusunan Tugas Akhir yang telah diselesaikan ini masih tidak mendekati kata sempurna. Maka dari itu penulis meminta kritik, masukan, serta ide yang dapat digunakan oleh penulis agar penyusunan Tugas Akhir akan menjadi jauh lebih baik lagi di masa mendatang.

Palembang, 27 Juni 2022

Penulis,

Muhammad Robby Bahari
NIM. 09011381823099

BRUTE FORCE ATTACK PATTERN VISUALIZATION USING K-NEAREST NEIGHBOR METHOD

Muhammad Robby Bahari (09011381823099)
Department of Computer Engineering, Faculty of Computer Science, Sriwijaya University
Email : robbybahari2467@gmail.com

ABSTRACT

Brute Force is one of the most frequently used methods by hackers in cyber crimes. To find out which variable features have the most significant role in the brute force dataset, it is necessary to implement feature selection. This final project discusses the visualization of brute force attack patterns using several feature selection methods, namely Random Forest Classifier (RFC), Mutual Information Classifier (MIC), Correlation Based Selection (CBS), and also Lasso Regularization Regression (LRR) and then classification using K-Nearest Neighbor algorithm to determine accuracy, precision, recall, and also F1-score. The data used in this study is CIC-IDS 2017 which is sourced from the Canadian Institute Cybersecurity. From the research conducted, it is found that the Random Forest Classifier feature selection produces the best accuracy, precision, recall, and F1-score among the others.

Keywords : Brute Force, Machine Learning, K-Nearest Neighbor, Feature Selection.

Palembang, 27 June 2022

Supervisor 1

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

Supervisor 2

Adi Hermansyah, M.T.
NIK. 1613033004890001

Acknowledged,
Head of Computer Systems Department

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

VISUALISASI POLA SERANGAN *BRUTE FORCE* MENGGUNAKAN METODE K-NEAREST NEIGHBOR

Muhammad Robby Bahari (09011381823099)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : robbybahari2467@gmail.com

ABSTRAK

Brute Force merupakan salah satu metode yang paling sering digunakan oleh para peretas dalam kejahatan dunia *cyber*. Untuk mengetahui fitur variabel yang paling berperan besar dalam dataset *brute force* maka diperlukan penerapan seleksi fitur. Penelitian tugas akhir ini membahas tentang visualisasi pola serangan *brute force* menggunakan beberapa metode *feature selection* yaitu *Random Forest Classifier* (RFC), *Mutual Information Classifier* (MIC), *Correlation Based Selection* (CBS), dan juga *Lasso Regularization Regression* (LRR) dan kemudian klasifikasi menggunakan algoritma K-Nearest Neighbor untuk mengetahui akurasi, presisi, *recall*, dan juga F1-score. Adapun data yang digunakan dalam penelitian ini adalah CIC-IDS 2017 yang bersumber dari *Canadian Institute Cybersecurity*. Dari penelitian yang dilakukan diperoleh hasil bahwa *feature selection Random Forest Classifier* menghasilkan akurasi, presisi, *recall*, dan F1-score yang paling baik diantara yang lain.

Kata Kunci : *Brute Force*, *Machine Learning*, K-Nearest Neighbor, *Feature Selection*.

Palembang, 27 Juni 2022

Pembimbing 1 Tugas Akhir	**Pembimbing 2 Tugas Akhir**
Ahmad Heryanto S.Kom, M.T.	**Adi Hermansyah, M.T.**
NIP. 198701222015041002	**NIK. 1613033004890001**

Mengetahui,
Ketua Jurusan Sistem Komputer

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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Penggunaan internet dalam kehidupan manusia tentunya tidak luput dari hal – hal yang bersifat pribadi dan privasi contohnya seperti media sosial, internet banking, dll. Orang yang tidak bertanggung jawab memiliki banyak cara untuk meretas akun dan mendapatkan data – data yang bersifat sensitif milik orang lain salah satunya adalah dengan metode *brute force.* Pada September 2017, McAffee melaporkan sekitar 20% dari total metode serangan yang digunakan oleh para peretas adalah metode *brute force* [1]. Sebagai salah satu metode yang paling sering digunakan dalam dunia *cyber* [2], serangan *brute force* dapat mengancam hampir apapun mulai dari *online banking*, *bitcoin wallet*, telnet server, dan bahkan institusi pemerintahan [1], [3], [4]. Banyak bahan ataupun alat yang dapat digunakan untuk melancarkan serangan *brute force* baik dengan berbagai tujuan contohnya seperti Aircrack-ng, L0phtCrack, Hashcat, dll. Serangan *brute force* dapat dilakukan baik melalui sistem operasi Windows maupun Linux, sehingga menjadikannya sebagai salah satu metode serangan yang paling mudah untuk dilakukan. Serangan *brute force* dilakukan dengan cara mengirimkan beberapa kombinasi kata – kata yang bertujuan untuk mendapatkan *password* yang sebenarnya dalam beberapa percobaan tersebut. Pada dasarnya serangan *brute force* akan meninggalkan pola serangan dan juga pola data [5]. KNN adalah suatu metode *machine learning* yang biasa dan dapat digunakan dalam melakukan klasifikasi *attack pattern* yang ditinggalkan oleh serangan *brute force*. KNN sangatlah penting dan dapat digunakan dalam *complex detection*, *link discovery*, *visualization*, dan juga *prediction* [6]. Metode KNN dipilih dalam penelitian karena kepopuleran penggunaannya dalam data *mining* dan *statistic* serta kemudahan implementasi dan performa klasifikasi yang optimal [7].

Attack Pattern yang dihasilkan oleh serangan *brute force* akan dimasukkan dan kemudian diolah oleh algoritma K-Nearest Neighbor sebelum pada akhirnya di visualisasikan. Diharapkan dengan adanya pemahaman mengenai visualisasi pola serangan *brute force* akan meningkatkan keamanan portal login yang ada di internet.

Penelitian mengenai *brute force* sudah banyak dibahas sebelumnya, salah satunya pada jurnal dengan judul "***Classification of SSH Attacks using Machine Learning Algorithms***"[8]. Jurnal tersebut membahas tentang pengklasifikasian serangan SSH *brute force* dengan metode membandingkan beberapa algoritma *machine learning* yaitu *Naïve Bayes*, *J48 Decision Tree*, *Logistic Regression* dan *Support Vector Machine* (SVM). Hasilnya didapatkan bahwa keempat metode tersebut menunjukkan tingkat akurasi sekitar 99% yang menunjukkan bahaya dari serangan SSH *brute force*. Namun dalam hal sensitivitas, hanya metode *decision tree* yang memiliki tingkat akurasi sebesar 92,86% dibandingkan dengan ketiga metode lainnya yaitu dengan sensitivitas sekitar 57,14% [8].

Penelitian lainnya mengenai *brute force* telah dibahas pada jurnal yang berjudul "***Data Analytics for Modeling and Visualizing Attack Behaviors: A Case Study on SSH Brute Force Attacks***"[9]. Jurnal tersebut membahas tentang visualisasi model *attack pattern* dari *brute force* menggunakan dua metode algoritma *unsupervised learning* yaitu *Self-Organizing Map* (SOM) dan *Association Rule Mining* (ARM) untuk memodelkan dan memvisualisasikan perilaku aliran jaringan dari sebuah *host* dengan menggabungkan beberapa *dataset*. Hasil penelitian didapatkan bahwa serangan *brute force* SSH memiliki pola perilaku mereka masing – masing yang berbeda dari pola perilaku arus lalu lintas jaringan SSH normal. Adapun kelemahan dari penelitian tersebut adalah tidak adanya sebuah sistem yang dapat mendeteksi serangan SSH *brute force* dengan tingkat akurasi yang dan juga tingkat *false alarm* yang rendah [9].

Adapun penelitian lain mengenai *brute force* dibahas pada jurnal yang berjudul "***A Brute-force CNN Model Selection for Accurate Classification of Sensorimotor Rhythms in* BCIs**" [10]. Jurnal tersebut membahas tentang penelitan megenai BCI (*Brain-Computer Interface*) yang mana memungkinkan orang dengan disabilitas untuk berinteraksi dengan lingkungan sekitarnya

menggunakan terjemahan dari citra mental mereka. Penelitian tersebut menggunakan *Electroencephalographic* (EEG) sebagai pola dasar dan metode *deep learning Convolutional Neural Network* (CNN). Hasilnya didapatkan bahwa EEGNet menunjukkan kinerja yang mutakhir dalam beberapa tugas klasifikasi EEG pada berbagai paradigma BCI, namun untuk kapasitas dan efisiensi dari EEGNet yang digunakan sebagai tolak ukur untuk perbandingan itu sendiri tidak diketahui [10].

Berdasarkan uraian latar belakang diatas, maka penulis menulis sebuah tugas akhir yang berjudul "**Visualisasi Pola Serangan *Brute Force* Menggunakan Metode K-Nearest Neighbor**".

1.2. Perumusan Masalah

Penelitian mengenai *brute force* sudah banyak dilakukan sebelumnya, mulai dari prediksi, deteksi, dan juga visualisasi. Berbagai metode juga sudah digunakan dalam penelitian – penelitian tersebut seperti Naïve Bayes, K-Mean, dll. Maka dengan demikian adapun perumusan masalah dalam penelitian ini adalah bagaimana cara penggunaan algoritma metode K-Nearest Neighbor (KNN) dalam permasalahan klasifikasi dan visualisasi serangan *brute force*.

1.3. Tujuan Penelitian

Adapun tujuan penelitian dari penyusunan tugas akhir ini, yaitu :

1. Melakukan klasifikasi serangan *brute force* menggunakan metode K-Nearest Neighbor.
2. Melakukan visualisasi pola serangan *brute force* menggunakan diagram garis *parallel coordinates*.
3. Mencari tingkat akurasi terbaik dari beberapa metode *feature selection* yang akan digunakan.

1.4. Manfaat

Adapun manfaat dari penyusunan tugas akhir, yaitu :

1. Visualisasi serangan *brute force* menggunakan metode K-Nearest Neighbor dapat memberikan hasil akurasi yang optimal.
2. Dapat memberikan informasi mengenai metode K-Nearest Neighbor dan pengaplikasiannya dalam visualisasi serangan *brute force*.
3. Dapat memberikan informasi mengenai dataset *brute force* yang digunakan dalam penelitian.

1.5. Batasan Masalah

Batasan masalah merupakan batasan yang digunakan dalam penelitian agar penelitian tidak melenceng terlalu jauh. Dengan demikian, batasan masalah dari penyusunan tugas akhir ini, yaitu :

1. Penelitian menggunakan dataset dari CICIDS 2017.
2. Penelitian menggunakan *software* Jupyter Notebook.
3. Algoritma klasifikasi yang digunakan dalam penelitian adalah algoritma K-Nearest Neighbor.
4. Visualisasi pola data dilakukan dengan menggunakan diagram garis *Parallel Coordinates*.

1.6. Sistematika Penulisan

Adapun penyusunan penulisan tugas akhir disusun menjadi beberapa sub bab yang akan dijelaskan secara rinci dan mengenai apa saja yang dilakukan oleh penulis pada saat melakukan penelitian. Secara sistematis, tugas akhir ini disusun sebagai berikut:

BAB I – PENDAHULUAN

Pada bagian **BAB I** berisi tentang latar belakang, hingga tujuan dan manfaat, serta perumusan masalah dan juga sistematika penulisan pada tugas akhir.

BAB II – TINJAUAN PUSTAKA

Pada bagian **BAB II** berisikan tentang informasi seperti penelitian terdahulu yang telah dilakukan oleh peneliti – peneliti sebelumnya, kajian literatur, serta juga terdapat landasan teori dari berbagai bahasan yang berhubungan dengan tema.

BAB III – METODOLOGI PENELITIAN

Pada bagian **BAB III** berisikan tentang informasi pengumpulan data, spesifikasi *hardware* dan *software* yang digunakan, serta juga terdapat metode dan *flowchart* yang digunakan dalam penelitian.

BAB IV – PEMBAHASAN

BAB IV berisikan tentang pembahasan inti dari riset yang telah diselesaikan serta juga berisi mengenai analisis hasil dari riset tersebut.

BAB V – PENUTUP

Bagian **BAB V** yang merupakan bab akhir berisikan tentang seperti kesimpulan dan saran.

DAFTAR PUSTAKA

[1] S. Salamatian, W. Huleihel, A. Beirami, A. Cohen, and M. Medard, "Why botnets work: Distributed brute-force attacks need no synchronization," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 9, pp. 2288–2299, 2019, doi: 10.1109/TIFS.2019.2895955.

[2] S. Salamatian, W. Huleihel, A. Beirami, A. Cohen, and M. Medard, "Centralized vs Decentralized Targeted Brute-Force Attacks: Guessing with Side-Information," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, no. c, pp. 3749–3759, 2020, doi: 10.1109/TIFS.2020.2998949.

[3] S. F. Tan and A. Samsudin, "Enhanced security of internet banking authentication with extended honey encryption (Xhe) scheme," *Stud. Comput. Intell.*, vol. 741, no. February 2019, pp. 201–216, 2018, doi: 10.1007/978-3-319-66984-7_12.

[4] 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*, no. November, pp. 379–385, 2014, doi: 10.1109/BIBE.2014.73.

[5] 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.

[6] X. Li, "DURS: A distributed method for k-nearest neighbor search on uncertain graphs," *Proc. - IEEE Int. Conf. Mob. Data Manag.*, vol. 2019-June, no. Mdm, pp. 377–378, 2019, doi: 10.1109/MDM.2019.00-23.

[7] S. Zhang *et al.*, "IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS 1 Efficient kNN Classification With Different Numbers of Nearest Neighbors," *Ieee Trans. Neural Networks Learn. Syst.*, pp. 1–12, 2017, [Online]. Available: http://ieeexplore.ieee.org.

[8] G. K. Sadasivam, C. Hota, and B. Anand, “Classification of SSH attacks using machine learning algorithms,” *2016 6th Int. Conf. IT Converg. Secur. ICITCS 2016*, 2016, doi: 10.1109/ICITCS.2016.7740316.

[9] C. Yao, X. Luo, and A. N. Zincir-Heywood, “Data analytics for modeling and visualizing attack behaviors: A case study on SSH brute force attacks,” *2017 IEEE Symp. Ser. Comput. Intell. SSCI 2017 - Proc.*, vol. 2018-Janua, pp. 1–8, 2018, doi: 10.1109/SSCI.2017.8280913.

[10] B. Abibullaev, I. Dolzhikova, and A. Zollanvari, “A Brute-Force CNN Model Selection for Accurate Classification of Sensorimotor Rhythms in BCIs,” *IEEE Access*, vol. 8, pp. 101014–101023, 2020, doi: 10.1109/ACCESS.2020.2997681.

[11] 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.

[12] 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.

[13] 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.

[14] M. Idhom, H. E. Wahanani, and A. Fauzi, “Network security system on multiple servers against brute force attacks,” *Proceeding - 6th Inf. Technol. Int. Semin. ITIS 2020*, pp. 258–262, 2020, doi: 10.1109/ITIS50118.2020.9321108.

[15] M. D. Hossain, H. Ochiai, F. Doudou, and Y. Kadobayashi, “SSH and FTP brute-force attacks detection in computer networks: Lstm and machine learning approaches,” *2020 5th Int. Conf. Comput. Commun. Syst. ICCCS 2020*, pp. 491–497, 2020, doi: 10.1109/ICCCS49078.2020.9118459.

[16] L. Bosnjak, J. Sres, and B. Brumen, “Brute-force and dictionary attack on

hashed real-world passwords," *2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2018 - Proc.*, no. May 2018, pp. 1161–1166, 2018, doi: 10.23919/MIPRO.2018.8400211.

[17] S. Zhang, X. Xie, and Y. Xu, "A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity," *IEEE Access*, vol. 8, pp. 128250–128263, 2020, doi: 10.1109/ACCESS.2020.3008433.

[18] S. Khan, S. Anjum, U. A. Gulzari, T. Umer, and B. S. Kim, "Bandwidth-Constrained Multi-Objective Segmented Brute-Force Algorithm for Efficient Mapping of Embedded Applications on NoC Architecture," *IEEE Access*, vol. 6, no. c, pp. 11242–11254, 2017, doi: 10.1109/ACCESS.2017.2778340.

[19] 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. XX, pp. 1–1, 2021, doi: 10.1109/access.2021.3126535.

[20] W. N. Fatihah Wan Mustapha, M. A. Abdul Aziz, M. Masrie, R. Sam, and M. N. M. Tan, "WiFi Approximated Strength Measurement Method with Brute Force Algorithm for a Minimum Number of AP and Maximum WiFi Coverage," *ISCAIE 2020 - IEEE 10th Symp. Comput. Appl. Ind. Electron.*, pp. 180–185, 2020, doi: 10.1109/ISCAIE47305.2020.9108833.

[21] S. Bhowal, S. R. Dutta, and S. Mitra, "An efficient reduced set brute force attack technique for a particular steganographic tool using vername algorithm," *2017 4th Int. Conf. Image Inf. Process. ICIIP 2017*, vol. 2018-January, pp. 133–136, 2018, doi: 10.1109/ICIIP.2017.8313698.

[22] 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, doi: 10.7753/IJCATR1001.1008.

[23] R. Z. Mahmood and A. F. Fathil, "High Speed Parallel RC4 Key Searching Brute Force Attack Based on FPGA," *2019 Int. Conf. Adv. Sci. Eng. ICOASE 2019*, pp. 129–134, 2019, doi: 10.1109/ICOASE.2019.8723737.

[24] S. M. Raafat and D. J. Naji, “Intelligent Optimized Controlled Health Care System Using Brute Force and Heuristic Algorithms,” *2018 3rd Sci. Conf. Electr. Eng. SCEE 2018*, pp. 134–139, 2018, doi: 10.1109/SCEE.2018.8684216.

[25] K. S. M. Moe and T. Win, “Enhanced honey encryption algorithm for increasing message space against brute force attack,” *ECTI-CON 2018 - 15th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol.*, pp. 86–89, 2019, doi: 10.1109/ECTICon.2018.8620050.

[26] W. G. Ho, C. S. Ng, N. A. Kyaw, N. Kyaw Zwa Lwin, K. S. Chong, and B. H. Gwee, “High Efficiency Early-Complete Brute Force Elimination Method for Security Analysis of Camouflage IC,” *Proc. 2020 IEEE Asia Pacific Conf. Circuits Syst. APCCAS 2020*, pp. 161–164, 2020, doi: 10.1109/APCCAS50809.2020.9301666.

[27] S. S. Kolahi, K. Treseangrat, and B. Sarrafpour, “Analysis of UDP DDoS flood cyber attack and defense mechanisms on Web Server with Linux Ubuntu 13,” *2015 Int. Conf. Commun. Signal Process. Their Appl. ICCSPA 2015*, 2015, doi: 10.1109/ICCSPA.2015.7081286.

[28] 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.

[29] Z. Tian, H. Qiao, J. Tian, H. Zhu, and X. Li, “An Automated Brute Force Method Based on Webpage Static Analysis,” *Proc. - 10th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2018*, vol. 2018-Janua, pp. 100–103, 2018, doi: 10.1109/ICMTMA.2018.00031.

[30] M. Andrus, S. Dean, T. K. Gilbert, N. Lambert, and T. Zick, “AI Development for the Public Interest: From Abstraction Traps to Sociotechnical Risks,” *Int. Symp. Technol. Soc. Proc.*, vol. 2020-Novem, no. Fair ML, pp. 72–79, 2020, doi: 10.1109/ISTAS50296.2020.9462193.

[31] Di. C. Nguyen *et al.*, “Enabling AI in Future Wireless Networks: A Data Life Cycle Perspective,” *IEEE Commun. Surv. Tutorials*, vol. 23, no. 1, pp. 553–595,

2021, doi: 10.1109/COMST.2020.3024783.

[32] M. P. Hosseini, A. Hosseini, and K. Ahi, “A Review on Machine Learning for EEG Signal Processing in Bioengineering,” *IEEE Rev. Biomed. Eng.*, vol. 14, no. c, pp. 204–218, 2021, doi: 10.1109/RBME.2020.2969915.

[33] A. Shrestha and A. Mahmood, “Review of deep learning algorithms and architectures,” *IEEE Access*, vol. 7, pp. 53040–53065, 2019, doi: 10.1109/ACCESS.2019.2912200.

[34] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, “Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection,” *2016 Int. Conf. Platf. Technol. Serv. PlatCon 2016 - Proc.*, 2016, doi: 10.1109/PlatCon.2016.7456805.

[35] Q. Liu and C. Liu, “A Novel Locally Linear KNN Method with Applications to Visual Recognition,” *IEEE Trans. Neural Networks Learn. Syst.*, vol. 28, no. 9, pp. 2010–2021, 2017, doi: 10.1109/TNNLS.2016.2572204.

[36] K. M. Thilina, K. W. Choi, N. Saquib, and E. Hossain, “Pattern classification techniques for cooperative spectrum sensing in cognitive radio networks: SVM and W-KNN approaches,” *GLOBECOM - IEEE Glob. Telecommun. Conf.*, pp. 1260–1265, 2012, doi: 10.1109/GLOCOM.2012.6503286.

[37] F. Zhao and Q. Tang, “A KNN learning algorithm for collusion-resistant spectrum auction in small cell networks,” *IEEE Access*, vol. 6, no. c, pp. 45796–45803, 2018, doi: 10.1109/ACCESS.2018.2861840.

[38] J. Vieira, R. P. Duarte, and H. C. Neto, “Knn-stuff: Knn streaming unit for fpgas,” *IEEE Access*, vol. 7, pp. 170864–170877, 2019, doi: 10.1109/ACCESS.2019.2955864.

[39] W. Xing and Y. Bei, “Medical Health Big Data Classification Based on KNN Classification Algorithm,” *IEEE Access*, vol. 8, pp. 28808–28819, 2020, doi: 10.1109/ACCESS.2019.2955754.

[40] P. Prathanrat and C. Polprasert, “Performance Prediction of Jupyter notebook in JupyterHub using Machine Learning,” *2018 Int. Conf. Intell. Informatics*

Biomed. Sci., vol. 3, pp. 157–162, 2018.

[41] J. Wang and A. Zeller, "Better Code , Better Sharing : On the Need of Analyzing Jupyter Notebooks," no. 3.

[42] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[43] K. R. Pushpalatha and A. G. Karegowda, "CFS Based Feature Subset Selection for Enhancing Classification of Similar Looking Food Grains-A Filter Approach," *2017 2nd Int. Conf. Emerg. Comput. Inf. Technol. ICECIT 2017*, pp. 1–6, 2018, doi: 10.1109/ICECIT.2017.8453403.