DETEKSI SERANGAN *TROJAN METASPLOIT* PADA ANDROID DENGAN METODE *SUPPORT VECTOR MACHINE (SVM)*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

M. AFIF ILDIANSYAH

09011182025022

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI SERANGAN *TROJAN METASPLOIT* PADA ANDROID DENGAN METODE *SUPPORT VECTOR MACHINE (SVM)*

SKRIPSI

Diajukan Untuk Melengkapi Salah
Satu Syarat Memperoleh Gelar
Sarjana Komputer

Oleh :

M. AFIF ILDIANSYAH

09011182025022

Indralaya, 16 Agustus 2024

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Jr. Sukemi, M.T.	Prof. Deris Stiawan, M.T.
NIP. 196612032006041001	NIP. 197806172006041002

AUTHENTICATION PAGE

METASPLOIT TROJAN ATTACKS DETECTION ON ANDROID USING THE *SUPPORT VECTOR MACHINE (SVM)* METHOD

SKRIPSI

Submitted To Complete One Of The
Requirements For Obtaining A
Bachelor's Degree in Computer
Science

By :
M. AFIF ILDIANSYAH
09011182025022

Indralaya, 16 Agustus 2024
Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. Sukemi, M.T.	**Prof. Deris Stiawan, M.T.**
NIP. 196612032006041001	**NIP. 197806172006041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 23 Juli 2024

Tim Penguji :

1. Ketua : Aditya P.P. Prasetyo. M.T.
2. Sekretaris : Nurul Afifah, M.Kom.
3. Penguji : Huda Ubaya, M.T.
4. Pembimbing : Prof. Deris Stiawan, M.T., PH.D.

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang Bertanda Tangan Di Bawah Ini :

Nama : M. Afif Ildiansyah

NIM : 09011182025022

Judul : DETEKSI SERANGAN *TROJAN METASPLOIT* PADA ANDROID DENGAN METODE *SUPPORT VECTOR MACHINE (SVM)*

Hasil Pengecekan Software iThenticate/Turnitin : 13%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya saya 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, 7 Agustus 2024
Penulis,

M. Afif Ildiansyah
NIM.09011182025022

KATA PENGANTAR

Segala puji syukur saya persembahkan kepada Allah Swt. karena berkat rahmat, rezeki dan hidayah-Nya penulis dapat menyelesaikan Tugas Akhir yang berjudul "**DETEKSI SERANGAN *TROJAN METASPLOIT* PADA ANDROID DENGAN METODE *SUPPORT VECTOR MACHINE (SVM)*"** ini dengan sebaik-baiknya. Tugas akhir ini dibuat dengan tujuan memenuhi syarat salah satu mata kuliah Kerja Praktek pada jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Indralaya,

Dalam laporan ini Penulis bertujuan untuk memberikan pemahaman yang lebih dalam tentang serangan payload pada perangkat Android dengan fokus pada deteksi *traffic* yang dihasilkan berdasarkan data. Dengan menggunakan metode *Support Vector Machine*, penelitian ini berusaha untuk mendeteksi data yang terkena serangan Trojan Metasploit.

Dalam penyusunan Tugas Akhir ini tidak terlepas dari bimbingan dan bantuan dari berbagai pihak hingga selesainya Tugas Akhir ini. Oleh karena itu dalam kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Allah SWT, atas berkat, rahmat dan karunia-Nya yang telah diberikan kepada penulis, sehingga penulis dapat menyelesaikan Tugas Akhir ini dalam keadaan yang berjalan baik dan lancar.
2. Kedua orang tua saya yang telah memberikan doa, dukungan dan juga semangat kepada penulis selama ini.
3. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya dan Dosen Akademik yang telah memberikan banyak ilmu
4. Bapak Prof. Deris Stiawan, M.T. selaku Dosen Pembimbing Tugas Akhir yang telah memberikan banyak ilmu dan membimbing dalam pengerjaan Tugas Akhir ini

Deteksi Serangan *Trojan Metasploit* Pada Android Dengan Metode *Support Vector Machine (SVM)*
M. Afif Ildiansyah

5. Orang-orang tersayang, saudara tak sedarah, serta sahabat di luar lingkungan kampus yang selalu memberikan semangat, dukungan dan motivasi dalam menyelesaikan laporan ini
6. Dan semua pihak yang telah membantu penulis.

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

.

Palembang, 7 Agustus 2024
Penulis,

M. AFIF ILDIANSYAH
NIM. 09011182025022

DETEKSI SERANGAN *TROJAN METASPLOIT* PADA ANDROID DENGAN METODE *SUPPORT VECTOR MACHINE* (*SVM*)

M. AFIF ILDIANSYAH
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : m.afif10318@gmail.com

ABSTRAK

Support Vector Machine (SVM) adalah algoritma pembelajaran mesin yang termasuk dalam kategori supervised learning. SVM bekerja dengan membangun *hyperplane* optimal yang memisahkan dua kelas dalam ruang fitur. Hyperplane ini dipilih sedemikian rupa sehingga memiliki margin maksimum, yaitu jarak terbesar antara titik-titik data dari kedua kelas. Selain *hyperplane, hyperparameter* juga merupakan salah satu hal yang perlu diperhatikan dalam metode ini. Dataset berasal dari percobaan hasil riset COMNETS. Support Vector Machine berhasil mengklasifikasikan traffic jaringan *malware* dan *benign*. Dengan evaluasi model menggunakan Confusion Matrix dan optimisasi *hyperparameter* menggunakan metode *Gridsearch CV*, model mampu memberikan performa deteksi yang baik dengan memperoleh akurasi sebesar 89,37%.

Kata kunci : *Support Vector Machine, Cyber Attack, Metasploit*

METASPLOIT TROJAN ATTACKS DETECTION ON ANDROID USING THE SUPPORT VECTOR MACHINE (SVM) METHOD

M. AFIF ILDIANSYAH
Department of Computer Systems, Faculty of Computer Science, Sriwijaya University
Email : m.afif10318@gmail.com

ABSTRACT

Support Vector Machine (SVM) is a machine learning algorithm that falls into the category of supervised learning. SVM works by constructing an optimal hyperplane that separates two classes in a feature space. This hyperplane is chosen in such a way that it has a maximum margin, which is the largest distance between data points from both classes. In addition to the hyperplane, hyperparameters are also one of the things that need to be considered in this method. The dataset comes from the COMNETS research experiment. Support Vector Machine successfully classifies malware and benign network traffic. With model evaluation using the Confusion Matrix and hyperparameter optimization using the Gridsearch CV method, the model is able to provide good detection performance by obtaining an accuracy of 89.37%.

Keyword : ***Support Vector Machine, Cyber Attack, Metasploit***

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam era yang didominasi oleh perangkat mobile, platform Android menjadi salah satu yang paling populer di dunia. Namun, popularitas ini juga membuatnya menjadi target yang menarik bagi para penyerang cyber[1]. Seiring dengan peningkatan pengguna Android, keamanan perangkat mobile menjadi semakin krusial. Salah satu ancaman yang meresahkan keamanan perangkat Android adalah serangan trojan, yang dapat merugikan pengguna dengan berbagai cara terutama yang menggunakan alat seperti Metasploit, telah menjadi ancaman serius terhadap keamanan perangkat Android[2].

Metasploit adalah sebuah platform penetration testing yang awalnya dikembangkan untuk membantu para profesional keamanan siber mengidentifikasi dan mengatasi kerentanan pada sistem komputer. Platform ini menyediakan kumpulan alat, eksploitasi, payload, dan modul serangan lainnya yang dapat digunakan secara etis untuk menguji keamanan suatu sistem[3]. Meskipun secara asli dirancang untuk keperluan uji penetrasi dan pengujian keamanan, sayangnya, sifat open-source dan keberadaan kode sumber Metasploit juga memberikan kemampuan kepada pihak yang tidak bertanggung jawab untuk memanfaatkannya sebagai alat yang mematikan[4]. Di sisi yang tidak etis, Metasploit dapat disalahgunakan sebagai alat yang kuat untuk merancang dan meluncurkan serangan siber yang merusak, termasuk di antaranya serangan trojan pada perangkat Android[5]. Dengan menggunakan modul-modul eksploitasi yang telah terintegrasi, para penyerang dapat mengeksploitasi celah keamanan pada perangkat Android, membuka pintu bagi akses yang tidak sah, pemantauan tanpa izin, atau pencurian data sensitif pengguna[6]. Seiring dengan meningkatnya kompleksitas serangan siber, deteksi dan perlindungan terhadap serangan trojan Metasploit pada platform Android menjadi semakin mendesak untuk mencegah dampak serius terhadap keamanan dan privasi pengguna[7]. Dalam penelitian ini, peneliti memusatkan perhatian pada eksekusi serangan Trojan Metasploit dengan fokus pada sistem keamanan. Dengan menerapkan teknik penetrasi dan eksploitasi yang

tersedia dalam Metasploit, serangan ini difokuskan pada pencapaian berhasilnya penetrasi pada perangkat Android sebagai objek studi utama. Pemanfaatan Metasploit diarahkan untuk melakukan infiltrasi pada perangkat Android dan menyisipkan kode berbahaya, memberikan kontrol sepenuhnya kepada penyerang terhadap perangkat tersebut. Penetrasi dalam konteks ini mencakup kemungkinan ekstraksi data pribadi, merusak fungsionalitas perangkat, atau bahkan menjalankan tindakan jahat lainnya.

Penggunaan Metode *Support Vector Machine (SVM)* dalam deteksi serangan trojan Metasploit didasarkan pada kemampuan klasifikasi yang sangat efektif dalam konteks klasifikasi biner (dua kelas). SVM dapat mengelompokkan data ke dalam dua kelas berdasarkan pola dan karakteristik yang dipelajari dari data latihan. SVM memiliki ketahanan terhadap outlier (data yang menyimpang dari pola umum). Dengan kata lain, SVM mampu meminimalkan dampak data yang tidak biasa atau ekstrem terhadap pembentukan model[8].

Berdasarkan latar belakang yang telah di uraikan diatas, maka penulis memutuskan untuk mengambil judul pada Tugas Akhir ini yaitu "**DETEKSI SERANGAN *TROJAN METASPLOIT* PADA ANDROID DENGAN METODE *SUPPORT VECTOR MACHINE (SVM)***".

1.2 Perumusan Masalah

Adapun perumusan masalah dalam laporan tugas akhir ini, yaitu :

1. Bagaimana cara mendeteksi serangan trojan Metasploit pada android dengan menggunakan metode *Support Vector Machine (SVM)*
2. Bagaimana performansi metode *Support Vector Machine (SVM)* dalam mendeteksi serangan trojan Metasploit pada android?

1.3 Tujuan Penelitian

Adapun tujuan dari penyusunan tugas akhir, yaitu:

1. Mengembangkan sebuah sistem deteksi serangan trojan metasploit pada android yang dapat mengidentifikasi *traffic* yang terinfeksi malware dengan akurasi yang tinggi.
2. Menerapkan metode Support Vector Machine (SVM) sebagai algoritma klasifikasi untuk mendeteksi antara *traffic* normal dan *traffic* malware berdasarkan fitur-fitur yang diekstraksi dari aplikasi android.

1.4 Manfaat Penelitian

Adapun manfaat dari penyusunan tugas akhir, yaitu:

1. Dapat dijadikan referensi untuk penelitian selanjutnya mengenai pencegahan serangan *Trojan Metasploit* pada android
2. Dapat meningkatkan pemahaman mengenai serangan *Trojan Metasploit*
3. Dapat mempelajari penggunaan metode *Support Vector Machine (SVM)* pada deteksi Malware

1.5 Batasan Masalah

Adapun batasan masalah dari penyusunan tugas akhir ini, yaitu:

1. Dataset yang digunakan adalah dataset yang dibuat dari hasil riset penelitian.
2. Metode yang digunakan pada penelitian ini hanya menggunakan *Support Vector Machine (SVM).*
3. Pada penelitian ini hanya membahas cara mendeteksi serangan *Trojan Metasploit* dan tidak membahas cara pencegahannya.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut :

1. Metode Studi Pustaka dan Literatur

   Pada metode ini, penulis melakukan pencarian dan pengumpulan referensi berupa literatur yang terdapat pada artikel, jurnal dan internet yang berkaitan dengan Tugas Akhir yang sedang dikerjakan.

2. Metode Konsultasi

   Pada metode ini dengan berbagai pihak lain diantaranya dosen dan praktisi

3. Pemrosesan Data

   Tahan ini dilakukan dengan membahas proses pengolahan data berbentuk file CSV.

4. Deteksi

   Tahap ini dilakukan dengan pengujian data yang sesuai dengan parameter-parameter serangan yang ditentukan oleh batasan masalah

5. Analisa dan Kesimpulan

   Tahap ini melakukan Analisa terhadap hasil yang sudah didapatkan sebelumnya. Selanjutnya ditarik kesimpulan dari permasalahan dan hasil tersebut

1.7 Sistematika Penulisan

Sistematika Penulisan yang dilakukan dalam Tugas Akhir ini adalah :

BAB I PENDAHULUAN

Pada bab pertama ini berisi mengenai uraian singkat tentang latar belakang, tujuan, manfaat, batasan masalah, metodologi penelitian serta sisitematika penulisan oleh penulis.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi tentang Studi Pustaka yang dimana terdapat jurnal-jurnal dan penjelasan yang terkait pada penelitian ini yang bertujuan untuk sebagai referensi dasar pada penelitian.

BAB III METODOLOGI PENELITIAN

Pada Bab ini menjelaskan berbagai fase yang dilakukan peneliti selama proses penelitian

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan hasil dan pembahasan dari penelitian yang telah dilakukan oleh penulis

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan yang diambil selama proses penelitian sebagai jawaban atas tujuan yang ingin dicapai, serta saran atas hasil yang diperoleh peneliti dari proses tugas akhir peneliti

DAFTAR PUSTAKA

[1] P. Bhat and K. Dutta, "A survey on various threats and current state of security in android platform," *ACM Comput. Surv.*, vol. 52, no. 1, 2019, doi: 10.1145/3301285.

[2] S. Raj and N. K. Walia, "A Study on Metasploit Framework: A Pen-Testing Tool," *2020 Int. Conf. Comput. Perform. Eval. ComPE 2020*, no. July 2020, pp. 296–302, 2020, doi: 10.1109/ComPE49325.2020.9200028.

[3] O. Valea and C. Oprisa, "Towards Pentesting Automation Using the Metasploit Framework," *Proc. - 2020 IEEE 16th Int. Conf. Intell. Comput. Commun. Process. ICCP 2020*, no. September 2020, pp. 171–178, 2020, doi: 10.1109/ICCP51029.2020.9266234.

[4] Y. Kolli, T. K. Mohd, and A. Y. Javaid, "Remote Desktop Backdoor Implementation with Reverse TCP Payload using Open Source Tools for Instructional Use," *2018 IEEE 9th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2018*, no. November, pp. 444–450, 2018, doi: 10.1109/IEMCON.2018.8614801.

[5] I. Journal, C. Science, and E. Volume-, "Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework Mujahid Tabassum Saju Mohanan Department of IT , University of Technology and Department of IT , University of Technology and Applied Sciences Applied Sciences Muscat , Oman Tripti ," no. 1, pp. 9–22, 2021.

[6] A. Dwivedi, "LAUNCHING AN ATTACK AND EXPLOITING THE ANDROID USING," vol. 1, no. 4, pp. 42–53, 2022.

[7] C. Du, S. Liu, L. Si, Y. Guo, and T. Jin, "Using object detection network for malware detection and identification in network traffic packets," *Comput. Mater. Contin.*, vol. 64, no. 3, pp. 1785–1796, 2020, doi: 10.32604/cmc.2020.010091.

[8] S. Huang, C. A. I. Nianguang, P. Penzuti Pacheco, S. Narandes, Y. Wang, and X. U. Wayne, "Applications of support vector machine (SVM) learning in cancer genomics," *Cancer Genomics and Proteomics*, vol. 15, no. 1, pp.

41–51, 2018, doi: 10.21873/cgp.20063.

[9] K. Liu, S. Xu, G. Xu, M. Zhang, D. Sun, and H. Liu, "A Review of Android Malware Detection Approaches Based on Machine Learning," *IEEE Access*, vol. 8, pp. 124579–124607, 2020, doi: 10.1109/ACCESS.2020.3006143.

[10] R. Mayrhofer, J. Vander Stoep, C. Brubaker, and N. Kralevich, "The Android Platform Security Model," *ACM Trans. Priv. Secur.*, vol. 24, no. 3, 2021, doi: 10.1145/3448609.

[11] P. Wang, J. Guo, and L. F. Li, "Machine learning model based on non-convex penalized huberized-SVM," *J. Electron. Sci. Technol.*, vol. 22, no. 1, p. 100246, 2024, doi: 10.1016/j.jnlest.2024.100246.

[12] W. An, B. Gao, J. Liu, J. Ni, and J. Liu, "Case Studies in Thermal Engineering Predicting hourly heating load in residential buildings using a hybrid SSA – CNN – SVM approach," vol. 59, no. April, 2024, doi: 10.1016/j.csite.2024.104516.

[13] S. Akil, S. Sekkate, and A. Adib, "Exploring machine learning techniques for oil price forecasting: A comparative study of SVM, SMO, and SGD-base models," *Procedia Comput. Sci.*, vol. 232, no. 2023, pp. 924–933, 2024, doi: 10.1016/j.procs.2024.01.092.

[14] S. Golla, B. Sujatha, and L. Sumalatha, "TIE- text information extraction from natural scene images using SVM," *Meas. Sensors*, vol. 33, no. February, p. 101018, 2024, doi: 10.1016/j.measen.2023.101018.

[15] M. Zhang, M. Treder, D. Marshall, and Y. Li, "Explaining the predictions of kernel SVM models for neuroimaging data analysis," *Expert Syst. Appl.*, vol. 251, no. March, p. 123993, 2024, doi: 10.1016/j.eswa.2024.123993.

[16] M. Li, K. Li, Y. Liu, S. Wu, Q. Qin, and R. Yue, "Goaf risk prediction based on IAOA–SVM and numerical simulation: A case study," *Undergr. Sp.*, vol. 15, pp. 153–175, 2024, doi: 10.1016/j.undsp.2023.07.003.

[17] A. Adekotujo, A. Odumabo, A. Adedokun, and O. Aiyeniko, "A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux,

Mac, Android and iOS," *Int. J. Comput. Appl.*, vol. 176, no. 39, pp. 16–23, 2020, doi: 10.5120/ijca2020920494.

[18] S. Garg and N. Baliyan, "Data on Vulnerability Detection in Android," *Data Br.*, vol. 22, pp. 1081–1087, 2019, doi: 10.1016/j.dib.2018.12.038.

[19] X. Chen *et al.*, "Android HIV: A Study of Repackaging Malware for Evading Machine-Learning Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 987–1001, 2020, doi: 10.1109/TIFS.2019.2932228.

[20] R. B. Joseph, M. F. Zibran, and F. Z. Eishita, "Choosing the weapon: A comparative study of security analyzers for android applications," *2021 IEEE/ACIS 19th Int. Conf. Softw. Eng. Res. Manag. Appl. SERA 2021*, no. March, pp. 51–57, 2021, doi: 10.1109/SERA51205.2021.9509271.

[21] R. Tahir, "A Study on Malware and Malware Detection Techniques," *Int. J. Educ. Manag. Eng.*, vol. 8, no. 2, pp. 20–30, 2018, doi: 10.5815/ijeme.2018.02.03.

[22] M. Yong Wong, M. Landen, M. Antonakakis, D. M. Blough, E. M. Redmiles, and M. Ahamad, "An Inside Look into the Practice of Malware Analysis," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 3053–3069, 2021, doi: 10.1145/3460120.3484759.

[23] T. J. L. Tan and R. Shokri, "Bypassing Backdoor Detection Algorithms in Deep Learning," *Proc. - 5th IEEE Eur. Symp. Secur. Privacy, Euro S P 2020*, pp. 175–183, 2020, doi: 10.1109/EuroSP48549.2020.00019.

[24] Y. Li, Y. Jiang, Z. Li, and S. T. Xia, "Backdoor Learning: A Survey," *IEEE Trans. Neural Networks Learn. Syst.*, pp. 1–17, 2022, doi: 10.1109/TNNLS.2022.3182979.

[25] D. Tang, X. Wang, and H. Tang, "Open access to the Proceedings of the 30th USENIX Security Symposium is sponsored by USENIX. Demon in the Variant: Statistical Analysis of DNNs for Robust Backdoor Contamination Detection Demon in the Variant: Statistical Analysis of DNNs for Robust Backd," 2021.

[26] R. Cayre *et al.*, "Mirage : towards a Metasploit-like framework for IoT To cite this version : HAL Id : hal-02346074 Mirage : towards a Metasploit-like framework for IoT," 2019.

[27] B. Mahesh, "Machine Learning Algorithms - A Review | Enhanced Reader," *Int. J. Sci. Res.*, vol. 9, no. 1, pp. 381–386, 2020, doi: 10.21275/ART20203995.

[28] Q. Bi, K. E. Goodman, J. Kaminsky, and J. Lessler, "What is machine learning? A primer for the epidemiologist," *Am. J. Epidemiol.*, vol. 188, no. 12, pp. 2222–2239, 2019, doi: 10.1093/aje/kwz189.

[29] M. A. K. Raiaan *et al.*, "A systematic review of hyperparameter optimization techniques in Convolutional Neural Networks," *Decis. Anal. J.*, vol. 11, no. April, p. 100470, 2024, doi: 10.1016/j.dajour.2024.100470.

[30] V. Hnamte and J. Hussain, "Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach," *Telemat. Informatics Reports*, vol. 11, no. July, p. 100077, 2023, doi: 10.1016/j.teler.2023.100077.

[31] Ž. Vujović, "Classification Model Evaluation Metrics," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 6, pp. 599–606, 2021, doi: 10.14569/IJACSA.2021.0120670.

[32] M. Zulfiqar, M. Kamran, M. B. Rasheed, T. Alquthami, and A. H. Milyani, "Hyperparameter optimization of support vector machine using adaptive differential evolution for electricity load forecasting," *Energy Reports*, vol. 8, pp. 13333–13352, 2022, doi: 10.1016/j.egyr.2022.09.188.

[33] A. A. Chowdhury, A. Das, K. K. S. Hoque, and D. Karmaker, "A Comparative Study of Hyperparameter Optimization Techniques for Deep Learning," no. January, pp. 509–521, 2022, doi: 10.1007/978-981-19-0332-8_38.