DETEKSI TROJAN METASPLOIT REVERSE TCP PADA NETWORK TRAFFIC DENGAN METODE K-NEAREST NEIGHBOR

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

NABILA SINTIA

09011282126073

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

DETEKSI TROJAN METASPLOIT REVERSE TCP PADA NETWORK TRAFFIC DENGAN METODE K-NEAREST NEIGHBOR

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

NABILA SINTIA

09011282126073

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI TROJAN METASPLOIT REVERSE TCP PADA NETWORK TRAFFIC DENGAN METODE K-NEAREST NEIGHBOR

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

NABILA SINTIA

09011282126073

Pembimbing 1	**: Prof. Ir. Deris Stiawan, M.T., Ph.D.** **NIP. 197806172006041002**
Pembimbing 2	**: Nurul Afifah., M.Kom.** **NIP. 199211102023212049**

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi., M.T.

196612032006041001

AUTHENTICATION PAGE

SKRIPSI

METASPLOIT REVERSE TCP TROJAN DETECTION ON NETWORK TRAFFIC WITH K-NEAREST NEIGHBOR METHOD

As one of the requirements for completing studies
in the S1 Computer Systems Study Program

By:

NABILA SINTIA

09011282126073

Advisor 1	**: Prof. Ir. Deris Stiawan, M.T., Ph.D.** **NIP. 197806172006041002**
Advisor 2	**: Nurul Afifah., M.Kom.** **NIP. 199211102023212049**

Approved by,

Head of Computer System Department

Dr. Ir. Sukemi., M.T.

196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Jum'at

Tanggal : 13 Juni 2025

Tim Penguji :

1. Ketua : Sutarno, M.T.
2. Penguji : Dr. Ir. Ahmad Heryanto, M.T.
3. Pembimbing I : Prof. Ir. Deris Stiawan, M.T., Ph.D.
4. Pembimbing II : Nurul Afifah, M.Kom

Mengetahui, 26/6/25

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Nabila Sintia

NIM : 09011282126073

Judul : Deteksi Trojan Metasploit Reverse TCP Pada Network Traffic Dengan Metode K-Nearest Neighbor

Hasil Pengecekan Software Turnitin : 5%

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

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

ng, 13 Juni 2025

Nabila Sintia

NIM. 09011282126073

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur atas kehadirat Allah SWT, karena berkat Rahmat dan Karunia-Nya lah sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul **"Deteksi Trojan Metasploit Reverse TCP Pada Network Traffic Dengan Metode K-Nearest Neighbor"**. Shalawat beriringkan salam senantiasa tercurahkan kepada Nabi Muhammad Shallallahu 'Alaihi Wasallam yang telah membawa kedamaian dan rahmat untuk semesta alam serta menjadi suri tauladan bagi umatnya.

Tujuan dari penelitian Tugas Akhir ini adalah untuk melengkapi salah satu syarat dalam memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian serta observasi dari berbagai sumber literatur yang mendukung dalam penulisan Tugas Akhir ini.

Selesainya penulisan Tugas Akhir ini tidak terlepas dari peran serta semua pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis selama penyelesaian Tugas Akhir
2. Cinta pertama dan panutanku, Ayahanda Endang Azhari dan pintu surgaku Ibunda Sutriani. Terimakasih atas segala pengorbanan, doa dan kasih sayang dengan penuh keikhlasan yang tak terhingga kepada penulis. Terimakasih selalu berjuang untuk kehidupan penulis.
3. Bapak Prof. 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 Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Prof. Ir. Deris Stiawan , M.T., PH.D. Selaku Dosen Pembimbing I Tugas Akhir.
6. Ibu Nurul Afifah., M.Kom. Selaku Dosen Pembimbing II Tugas Akhir

7. Bapak Dr. Rossi Passarella, M.ENG. Selaku Dosen Pembimbing Akademik
8. Kak Angga dan Mbak Sari selaku Admin Jurusan Sistem Komputer yang telah membantu administrasi dalam menyelesaikan Tugas Akhir
9. Kepada Saudari dan Keponakan penulis yang tak kalah penting kehadirannya. Terimakasih telah menjadi bagian dari perjalanan hidup penulis. Telah mendukung dan menghibur penulis dalam menyelesaikan Tugas Akhir.
10. Kepada teman seperjuangan riset malware android ririn febriana dan viona aulia meidy terima kasih sudah membantu dan menemani penulis selama menyelesaikan tugas akhir.
11. Kepada Defri Anugra terima kasih yang telah setia mendampingi dan memberikan semangat selama proses penyusunan skripsi ini. Kehadiran dan dukungannya sangat berarti bagi penulis.
12. Seluruh teman-teman seperjuangan Angkatan 2021 Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya

Penulis menyadari bahwa tugas akhir ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dikemudian hari.

Akhir kata dengan segala keterbatasan, penulis berharap semoga tugas akhir ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung maupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran dan penelitian.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, 13 Juni 2025
Penulis,

Nabila Sintia
NIM.09011282126073

DETEKSI TROJAN METASPLOIT REVERSE TCP PADA NETWORK TRAFFIC DENGAN METODE K-NEAREST NEIGHBOR

NABILA SINTIA (09011282126073)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: 09011282126073@student.unsri.ac.id

ABSTRAK

Android merupakan salah satu sistem operasi yang banyak digunakan. Perangkat Android menyimpan berbagai informasi pribadi dan sensitif yang berisiko menimbulkan ancaman keamanan. Salah satu ancaman utama adalah trojan *metasploit* teknik *reverse* TCP, yang memungkinkan penyerang mengontrol perangkat secara *remote*. Penelitian ini bertujuan untuk mendeteksi trojan metasploit *reverse* TCP pada *network traffic*. Penelitian ini menggunakan metode *K-Nearest Neighbor* (KNN) untuk klasifikasi dengan menentukan jumlah tetangga terdekat (k). *KNeighborCalssifer* digunakan untuk membuat dan melatih model dalam mendeteksi pola pada suatu data. Hasil penelitian menunjukan bahwa metode *K-Nearest Neighbor* (KNN) dengan seleksi fitur menggunakan *Feature Elimination* (RFE) efektif dalam menemukan fitur yang relevan. Penggunaan metode *K-Nearest Neighbor* (KNN) dengan RFE menghasilkan akurasi 97,29%, lebih tinggi dibandingkan model tanpa seleksi fitur yang hanya mencapai 95,66%, sehingga menunjukkan peningkatan performa dalam mendeteksi trojan *metasploit*.

Kata Kunci : *Android, Trojan, Metasploit, Reverse, K-Nearest Neighbor*

DETEKSI TROJAN METASPLOIT REVERSE TCP PADA NETWORK TRAFFIC DENGAN METODE K-NEAREST NEIGHBOR

NABILA SINTIA (09011282126073)

Department of Computer System, Faculty of Computer Science

Sriwijaya University

Email: 09011282126073@student.unsri.ac.id

ABSTRACT

Android is one of the most widely used operating systems. Android devices store various personal and sensitive information, which poses significant security risks. One of the major threats is the metasploit trojan using the reverse TCP technique, which allows attackers to remotely control the device. This study aims to detect the metasploit reverse TCP trojan in network traffic. The research utilizes the K-Nearest Neighbor (KNN) method for classification by determining the optimal number of nearest neighbors (k). The KNeighborsClassifier is used to build and train the model to detect patterns in the data. The results show that the K-Nearest Neighbor (KNN) method combined with feature selection using Recursive Feature Elimination (RFE) is effective in identifying relevant features. The use of KNN with RFE achieved an accuracy of 97.29%, which is higher than the model without feature selection, which only reached 95.66%, thus demonstrating improved performance in detecting Metasploit trojans.

Keywords: *Android, Trojan, Metasploit, Reverse, K-Nearest Neighbor*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Android menurut [1], merupakan salah satu sistem operasi (OS) yang paling banyak digunakan, menyediakan lingkungan pengembangan *open- source* yang dibangun di atas sistem operasi Linux. Perangkat android berdasarkan [2], menyediakan berbagai layanan, perangkat ini juga menyimpan sejumlah besar informasi pribadi dan sensitif, yang berisiko menimbulkan ancaman terhadap keamanan dan privasi penggunanya. Salah satu ancaman utama menurut [3], adalah serangan malware pada perangkat mobile, yang dapat digunakan untuk mencuri data penting, melacak aktivitas pengguna, serta melakukan tindakan yang tidak sah. Hal ini menunjukan pentingnya upaya mendeteksi dan mencegah malware pada perangkat android.

Malware *(Malicious Software)* menurut [4], adalah perangkat lunak berbahaya yang sering dimanfaatkan oleh penjahat siber untuk menjalankan muatan berbahaya ke perangkat pengguna, seperti komputer, smartphone dan jaringan komputer. Malware Android dapat muncul dalam berbagai bentuk, seperti virus, worm, spyware, ransomware dan trojan. Trojan menurut [5], adalah jenis malware yang menyamar sebagai perangkat lunak asli dan terinstal di komputer. Penyerang bisa menyembunyikan kode berbahaya ini di dalam program yang terlihat aman, seperti lampiran email atau aplikasi gratis yang diunduh.

Metasploit menurut [6], adalah framework yang digunakan untuk pengujian penetrasi dan eksploitasi keamanan jaringan. Framework ini menyediakan kumpulan alat untuk eksploitasi kerentanan, payload, dan modul serangan lainnya yang digunakan untuk menguji keamanan suatu sistem. Di sisi yang tidak etis, [7] menyebutkan Metasploit dimanfaatkan sebagai alat untuk merancang dan menjalankan serangan siber yang merugikan, seperti serangan trojan pada perangkat Android. Trojan metasploit sering dipilih oleh penjahat siber untuk meretas perangkat Android. Salah satu teknik yang digunakan Reverse TCP, dalam metasploit untuk menghubungkan perangkat target dengan server

penyerang, sehingga memungkinkan penyerang untuk menyisipkan payload dan mengontrol perangkat secara remote. Proses ini berdasarkan [8], melibatkan eksploitasi kerentanan pada sistem Android, di mana penyerang dapat memanfaatkan koneksi balik untuk melakukan aktivitas berbahaya, seperti mencuri data atau merusak sistem.

Pada penelitian ini [9], mendeteksi malware Android melalui teknik STAR (Systematic Malware Detection in Android). Penelitian ini mengelolah dataset CICMalDroid 2020, Drebin 4000, dan AndroZoo menggunakan PCA untuk ekstraksi fitur. Model machine learning yang digunakan dalam penelitian ini adalah pengklasifikasi ensemble seperti Bagging, AdaBoost, dan LogitBoost diterapkan dengan hasil menunjukkan akurasi 99,50%, serta peningkatan deteksi sebesar 4,34%, 1,41%, dan 2,52% dibandingkan metode ERBE, De-LADY, dan MSFDroid.

Pada penelitian ini [10], dibahas tentang penggunaan model machine learning untuk mendeteksi Remote Access Trojans (RAT) dalam lalu lintas jaringan menggunakan matriks transisi byte dan arsitektur CNN. Penelitian ini mencakup pengumpulan data dari tahap awal komunikasi, pengembangan model deteksi, dan evaluasi kinerja model.Hasil eksperimen menunjukkan bahwa metode yang diusulkan, RATMD, mencapai akurasi deteksi sebesar 95,5% dengan menggunakan byte sequence dari paket layanan TCP, yang lebih tinggi dibandingkan dengan model CNN lainnya seperti, VGG16 dan ResNet18, yang masing-masing memiliki akurasi 92% dan 93,8%.

Pada penelitian ini [11], dibahas tentang penggunaan algoritma machine learning untuk mendeteksi malware Android melalui analisis fitur statis yang berbasis pada izin dan panggilan API. Penelitian ini mencakup pemisahan dataset menjadi dua set fitur yang berbeda, yaitu fitur izin dan fitur panggilan API, serta penerapan pemilihan fitur penting menggunakan Recursive Feature Elimination (RFE) pada model regresi logistik. Hasil eksperimen menunjukkan bahwa classifier Support Vector Machine (SVM) mencapai tingkat akurasi deteksi sebesar 94% menggunakan fitur izin, dan 83% menggunakan fitur panggilan API. Selain itu, algoritma K-nearest neighbors (KNN) dan Naive Bayes (NB) juga

menunjukkan kinerja yang baik, dengan KNN mencapai akurasi 87,27% dan Naive Bayes mencapai akurasi 84,33%. Metode ini menunjukkan efektivitas dalam mendeteksi malware Android dengan memanfaatkan berbagai algoritma machine learning.

Berdasarkan ulasan dari beberapa penelitian, penulis melakukan deteksi trojan metasploit pada lalu lintas jaringan reverse tcp menggunakan dataset berformat pcap yang telah diekstraksi menjadi csv dan dianalisis dengan machine learning.Penelitian ini diusulkan dengan judul **"Deteksi Trojan Metasploit Reverse TCP Pada Network Traffic Dengan Metode K-Nearest Neighbor"**

1.2 Rumusan Masalah

Berdasarkan penulisan latar belakang masalah yang ada. Adapun permasalahan yang akan dibahas pada penelitian ini meliputi:

1. Bagaimana proses ekstraksi dataset dari trafik jaringan reverse TCP?
2. Bagaimana teknik seleksi fitur yang digunakan untuk memilih fitur yang relevan?
3. Bagaimana performa model k-nearest neighbor dalam mendeteksi trojan metasploit pada lalu lintas jaringan *reverse* TCP?

1.3 Batasan Masalah

Batasan masalah dalam penulisan penelitian tugas akhir ini adalah sebagai berikut:

1. Dataset yang digunakan oleh penulis dibuat di Laboratorium comnets Indralaya Universitas Sriwijaya
2. Penelitian ini hanya berfokus pada penggunaan RFE (*Recursive Feature Elimination*) untuk pemilihan fitur.
3. Deteksi trojan metasploit pada lalu lintas jaringan reverse TCP menggunakan algoritma K-Nearest Neighbor.
4. Penelitian ini hanya berfokus pada deteksi trojan metasploit pada lalu lintas jaringan reverse TCP, tanpa membahas deteksi malware jenis lain.

1.4 Tujuan

Adapun tujuan dari penulisan tugas akhir ini adalah sebagai berikut:

1. Melakukan ekstraksi dataset yang berbentuk .pcap menjadi .csv dengan menggunakan CICFlowMeter.
2. Menggunakan RFE (*Recursive Feature Elimination*) untuk seleksi fitur yang relevan dalam deteksi trojan metasploit pada *reverse* TCP.
3. Evaluasi performa K-Nearest Neighbor dalam mendeteksi trojan metasploit pada *reverse* TCP.

1.5 Manfaat

Adapun manfaat dari penulisan tugas akhir ini adalah sebagai berikut:

1. Memahami proses ekstraksi dataset menggunakan CICFlowMeter
2. Mengoptimalkan waktu proses komputasi dengan menggunakan fitur yang relevan.
3. Menganalisis performa model K-Nearest Neighbor dalam mendeteksi Trojan Metasploit pada lalu lintas jaringan reverse TCP.

1.6 Metode Penelitian

Metode yang digunakan dalam pembuatan tugas akhir yang akan melewati tahapan-tahapan berikut:

1. Studi Pustaka (Studi Literatur)

Metode ini digunakan untuk mencari referensi, termasuk buku dan jurnal yang diperlukan dan relevan dengan penelitian ini yang berjudul “Deteksi Trojan Metasploit Reverse TCP Pada Network Traffic Dengan Metode K-Nearest Neighbor**”.**

2. Perancangan sistem

Pada tahap ini berupa proses perancangan dan pembangunan sistem untuk mendeteksi trojan metasploit pada lalu lintas jaringan reverse TCP dengan menggunakan algoritma K-Nearest Neighbor.

3. Pengujian

Pada tahap ini dilakukan pengujian berdasarkan metode yang digunakan dalam penelitian dan metode-metode yang digunakan oleh penelitian sebelumnya, pengujian ini bertujuan untuk memastikan hasil yang didapat sesuai dengan konteks penelitian.

4. Analisa

Pada tahap ini dilakukan pengolahan dan analisis data yang diperoleh dari hasil pengujian sebelumnya untuk mendapatkan data yang akurat. Selanjutnya, hasil pengolahan ini dianalisis dengan tujuan mengidentifikasi kekurangan dalam perancangan sistem tersebut.

5. Kesimpulan dan Saran

Pada tahap ini berupa kesimpulan berdasarkan permasalahan, studi pustaka, metode penelitian dan analisis hasil yang membuat saran yang diharapkan dapat menjadi landasan baru serta untuk pengembangan penelitian selanjutnya.

1.7 Sistematika Penulisan

Adapun sistematis penulisan dalam Tugas Akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Pada bab I akan berisikan latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat serta metodologi penelitian dan sistematika penulisan dengan topik yang diangkat adalah “Deteksi Trojan Metasploit Reverse TCP Pada Network Traffic Dengan Metode K-Nearest Neighbor”

BAB II TINJAUAN PUSTAKA

Pada bab II ini berisikan mengenai studi literatur penelitian terdahulu, dasar teori trojan metasploit, reverse tcp, dan pendekatan machine learning dengan algoritma K-Nearest Neighbor yang berhubungan langsung dengan penelitian sebelumnya.

BAB III METODE PENELITIAN

Pada bab III berisikan bagaimana langkah-langkah yang diambil peneliti selama penelitian, tahapan perancangan, dan penerapan pendekatan atau metode penelitian.

BAB IV HASIL DAN ANALISA

Pada bab IV berisikan hasil pengujian yang telah dilakukan dalam mendeteksi trojan metasploit reverse tcp dengan metode k-nearest neighbor serta analisis hasil data yang didapatkan.

BAB V KESIMPULAN

Pada bab V berisikan kesimpulan tentang hasil pengujian yang telah dilakukan dan berisikan saran-saran untuk penelitian selanjutnya

DAFTAR PUSTAKA

[1] A. Mafakheri and S. Sulaimany, “Android malware detection through centrality analysis of applications network,” *Appl. Soft Comput.*, vol. 165, no. June, p. 112058, 2024, doi: 10.1016/j.asoc.2024.112058.

[2] A. Alzubaidi, “Recent Advances in Android Mobile Malware Detection: A Systematic Literature Review,” *IEEE Access*, vol. 9, pp. 146318–146349, 2021, doi: 10.1109/ACCESS.2021.3123187.

[3] N. Bala, A. Ahmar, W. Li, F. Tovar, A. Battu, and P. Bambarkar, “DroidEnemy: Battling adversarial example attacks for Android malware detection,” *Digit. Commun. Netw.*, vol. 8, no. 6, pp. 1040–1047, Dec. 2022, doi: 10.1016/j.dcan.2021.11.001.

[4] O. Aslan and A. A. Yilmaz, “A New Malware Classification Framework Based on Deep Learning Algorithms,” *IEEE Access*, vol. 9, pp. 87936–87951, 2021, doi: 10.1109/ACCESS.2021.3089586.

[5] M. F. Ab Razak, M. I. Jaya, Z. Ismail, and A. Firdaus, “Trojan Detection System Using Machine Learning Approach,” *Indones. J. Inf. Syst.*, vol. 5, no. 1, pp. 38–47, 2022, doi: 10.24002/ijis.v5i1.5673.

[6] O. Valea and C. Oprisa, “Towards Pentesting Automation Using the Metasploit Framework,” in *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)*, Cluj-Napoca, Romania: IEEE, Sep. 2020, pp. 171–178. doi: 10.1109/ICCP51029.2020.9266234.

[7] M. Tabassum, T. Sharma, and S. Mohanan, “Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework,” *Int. J. Innov. Comput. Sci. Eng. IJICSE*, vol. 2, no. 1, pp. 9–22, May 2021.

[8] D. Aprilliansyah, I. Riadi, and Sunardi, “Analysis of Remote Access Trojan Attack using Android Debug Bridge,” *IJID Int. J. Inform. Dev.*, vol. 10, no. 2, pp. 102–111, Feb. 2022, doi: 10.14421/ijid.2021.2839.

[9] A. Mohanraj and K. Sivasankari, “Android traffic malware analysis and detection using ensemble classifier,” *Ain Shams Eng. J.*, no. July, p. 103134, 2024, doi: 10.1016/j.asej.2024.103134.

[10] B. Pi, C. Guo, Y. Cui, G. Shen, J. Yang, and Y. Ping, “Remote access trojan traffic early detection method based on Markov matrices and deep learning,” *Comput. Secur.*, vol. 137, p. 103628, Feb. 2024, doi: 10.1016/j.cose.2023.103628.

[11] A. S. Shatnawi, Q. Yassen, and A. Yateem, “An Android Malware Detection Approach Based on Static Feature Analysis Using Machine Learning Algorithms,” *Procedia Comput. Sci.*, vol. 201, no. C, pp. 653–658, 2022, doi: 10.1016/j.procs.2022.03.086.

[12] F. E. Ayo, J. B. Awotunde, S. O. Folorunso, M. O. Adigun, and S. A. Ajagbe, “A genomic rule-based KNN model for fast flux botnet detection,”

Egypt. Inform. J., vol. 24, no. 2, pp. 313–325, Jul. 2023, doi: 10.1016/j.eij.2023.05.002.

[13] A. Al Saaidah *et al.*, "Enhancing malware detection performance: leveraging K-Nearest Neighbors with Firefly Optimization Algorithm," *Multimed. Tools Appl.*, Mar. 2024, doi: 10.1007/s11042-024-18914-5.

[14] S. Niveditha *et al.*, "Predicting Malware Classification and Family using Machine Learning: A Cuckoo Environment Approach with Automated Feature Selection," *Procedia Comput. Sci.*, vol. 235, no. 2023, pp. 2434–2451, 2024, doi: 10.1016/j.procs.2024.04.230.

[15] T. A. Assegie, "An Optimized KNN Model for Signature-Based Malware Detection," *Int. J. Comput. Eng. Res. Trends*, vol. 8, no. 2, pp. 46–49, 2021.

[16] S. Kumar, Shersingh, S. Kumar, and K. Verma, "Malware Classification Using Machine Learning Models," *Procedia Comput. Sci.*, vol. 235, pp. 1419–1428, 2024, doi: 10.1016/j.procs.2024.04.133.

[17] A. Pathak, U. Barman, and Th. S. Kumar, "Machine learning approach to detect android malware using feature-selection based on feature importance score," *J. Eng. Res.*, p. S2307187724000981, Apr. 2024, doi: 10.1016/j.jer.2024.04.008.

[18] A. Muzaffar, H. Ragab Hassen, M. A. Lones, and H. Zantout, "An in-depth review of machine learning based Android malware detection," *Comput. Secur.*, vol. 121, p. 102833, 2022, doi: 10.1016/j.cose.2022.102833.

[19] H. Alamro, W. Mtouaa, S. Aljameel, A. S. Salama, M. A. Hamza, and A. Y. Othman, "Automated Android Malware Detection Using Optimal Ensemble Learning Approach for Cybersecurity," *IEEE Access*, vol. 11, no. June, pp. 72509–72517, 2023, doi: 10.1109/ACCESS.2023.3294263.

[20] H.-J. Zhu, L.-M. Wang, S. Zhong, Y. Li, and V. S. Sheng, "A Hybrid Deep Network Framework for Android Malware Detection," *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 12, pp. 5558–5570, Dec. 2022, doi: 10.1109/TKDE.2021.3067658.

[21] H. Kauser.Sk and M. Anu.V, "A Hybrid Model for Android Malware Detection using Decision Tree and KNN," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 10, no. 1s, pp. 321–328, Dec. 2022, doi: 10.17762/ijritcc.v10i1s.5899.

[22] Y. Hong, Q. Li, Y. Yang, and M. Shen, "Graph based encrypted malicious traffic detection with hybrid analysis of multi-view features," *Inf. Sci.*, vol. 644, p. 119229, Oct. 2023, doi: 10.1016/j.ins.2023.119229.

[23] M. M. Abualhaj, A. A. Abu-Shareha, Q. Y. Shambour, A. Alsaaidah, S. N. Al-Khatib, and M. Anbar, "Customized K-nearest neighbors' algorithm for malware detection," *Int. J. Data Netw. Sci.*, vol. 8, no. 1, pp. 431–438, 2024, doi: 10.5267/j.ijdns.2023.9.012.

[24] R. Islam, M. I. Sayed, S. Saha, M. J. Hossain, and M. A. Masud, "Android malware classification using optimum feature selection and ensemble machine

learning," *Internet Things Cyber-Phys. Syst.*, vol. 3, no. January, pp. 100–111, 2023, doi: 10.1016/j.iotcps.2023.03.001.

[25] D. T. Dehkordy and A. Rasoolzadegan, "A new machine learning-based method for android malware detection on imbalanced dataset," vol. 80, pp. 24533–24554, 2021.

[26] S. Bashir, F. Maqbool, F. H. Khan, and A. S. Abid, "Hybrid machine learning model for malware analysis in android apps," *Pervasive Mob. Comput.*, vol. 97, p. 101859, Jan. 2024, doi: 10.1016/j.pmcj.2023.101859.

[27] K. Kong, L. Wang, Z. Zhang, Y. Li, D. Zhao, and J. Huang, "KFFPDet: Android malicious application detection system with assisted detection of adversarial samples," *Expert Syst. Appl.*, vol. 252, p. 124095, Oct. 2024, doi: 10.1016/j.eswa.2024.124095.

[28] I. Almomani, T. Almashat, and W. El-Shafai, "Maloid-DS: Labeled Dataset for Android Malware Forensics," *IEEE Access*, vol. 12, pp. 73481–73546, 2024, doi: 10.1109/ACCESS.2024.3400211.

[29] V. Syrris and D. Geneiatakis, "On machine learning effectiveness for malware detection in Android OS using static analysis data," *J. Inf. Secur. Appl.*, vol. 59, p. 102794, Jun. 2021, doi: 10.1016/j.jisa.2021.102794.

[30] D. O. Sahin, S. Akleylek, and E. Kilic, "LinRegDroid: Detection of Android Malware Using Multiple Linear Regression Models-Based Classifiers," *IEEE Access*, vol. 10, pp. 14246–14259, 2022, doi: 10.1109/ACCESS.2022.3146363.

[31] N. Pachhala, S. Jothilakshmi, and B. P. Battula, "Prediction of novel malware using hybrid convolution neural network and long short-term memory approach," *Int. J. Electr. Comput. Eng. IJECE*, vol. 14, no. 4, p. 4508, Aug. 2024, doi: 10.11591/ijece.v14i4.pp4508-4517.

[32] S. Poornima and R. Mahalakshmi, "Automated malware detection using machine learning and deep learning approaches for android applications," *Meas. Sens.*, vol. 32, no. May 2023, p. 100955, 2024, doi: 10.1016/j.measen.2023.100955.

[33] A. Rahman, G. Mustafa, A. Q. Khan, M. Abid, and M. H. Durad, "Launch of denial of service attacks on the modbus/TCP protocol and development of its protection mechanisms," *Int. J. Crit. Infrastruct. Prot.*, vol. 39, p. 100568, Dec. 2022, doi: 10.1016/j.ijcip.2022.100568.

[34] L. Shuai and S. Li, "Performance optimization of Snort based on DPDK and Hyperscan," *Procedia Comput. Sci.*, vol. 183, no. 2018, pp. 837–843, 2021, doi: 10.1016/j.procs.2021.03.007.

[35] A. Waleed, A. F. Jamali, and A. Masood, "Which open-source IDS? Snort, Suricata or Zeek," *Comput. Netw.*, vol. 213, p. 109116, Aug. 2022, doi: 10.1016/j.comnet.2022.109116.

[36] E. J. Alqahtani, R. Zagrouba, and A. Almuhaideb, "A Survey on Android Malware Detection Techniques Using Supervised Machine Learning," *2024*

6th Int. Conf. Softw. Defin. Syst. SDS 2024, vol. PP, pp. 110–117, 2024, doi: 10.1109/SDS.2019.8768729.

[37] K. Shaukat, S. Luo, and V. Varadharajan, "A novel machine learning approach for detecting first-time-appeared malware," *Eng. Appl. Artif. Intell.*, vol. 131, p. 107801, May 2024, doi: 10.1016/j.engappai.2023.107801.

[38] S. Zhou, T. Li, and Y. Li, "Recursive Feature Elimination Based Feature Selection in Modulation Classification for MIMO Systems," *Chin. J. Electron.*, vol. 32, no. 4, pp. 785–792, Jul. 2023, doi: 10.23919/cje.2021.00.347.

[39] V. Ghate and S. Hemalatha C, "A comprehensive comparison of machine learning approaches with hyper-parameter tuning for smartphone sensor-based human activity recognition," *Meas. Sens.*, vol. 30, p. 100925, Dec. 2023, doi: 10.1016/j.measen.2023.100925.

[40] M. AFIF ILDIANSYAH, "DETEKSI SERANGAN TROJAN METASPLOIT PADA ANDROID DENGAN METODE SUPPORT VECTOR MACHINE (SVM)," Universitas Sriwijaya, Palembang, 2024.