Jurnal Teknologi dan Sains Modern
https://journal.scitechgrup.com/index.php/jtsm

Vol. 1 (1), 2024, Hal. 9-18

Inovasi Pembelajaran Mesin untuk Deteksi Malware: Analisis Komprehensif dan Tinjauan Literatur

Samsidar[1], Syaiful Bachri M[1,*], Muhammad Atnang[1], Sahriani[1,], Nurhikmah Fajar[2]

[1] Program Studi Teknologi Informasi, Fakultas Sains Teknologi dan Kesehatan, Institut Sains Teknologi dan Kesehatan 'Aisyiyah Kendari
[2] Program Studi Teknik Komputer, Fakultas Teknik, Institut Teknologi dan Sains Muhammadiyah Kolaka Utara

*Correspondence: sbm@istekaisyiyah.ac.id

Abstrak

Penelitian tentang deteksi malware menggunakan pembelajaran mesin dan teknik deep learning telah menjadi topik yang menarik dalam beberapa tahun terakhir. Kombinasi fitur statis dan dinamik telah terbukti efektif dalam meningkatkan akurasi deteksi hingga 95%, sementara pendekatan ensemble learning juga menunjukkan peningkatan yang signifikan, mencapai akurasi hingga 97% untuk malware nol-hari. Implikasi temuan ini sangat penting dalam konteks keamanan siber, dengan kemampuan deteksi yang lebih baik dapat membantu melindungi sistem dan infrastruktur kritis dari serangan malware yang semakin canggih. Namun, ada beberapa batasan dalam penelitian ini, termasuk fokus yang terbatas pada tinjauan literatur dan tidak mencakup evaluasi eksperimental langsung. Oleh karena itu, penelitian lanjutan diperlukan untuk menguji metode ini pada dataset yang lebih beragam dan lingkungan operasional yang lebih realistis. Kontribusi dari penelitian ini terletak pada pengembangan solusi deteksi malware yang lebih efektif dan akurat menggunakan pendekatan pembelajaran mesin dan deep learning. Pertanyaan dan arah penelitian baru termasuk investigasi efektivitas metode dalam lingkungan produksi, pengembangan model hibrid yang menggabungkan pembelajaran mesin dengan teknik lain, serta eksplorasi penggunaan pembelajaran mesin untuk deteksi malware pada perangkat Internet of Things (IoT). Penelitian ini juga menyoroti pentingnya mempertimbangkan variabel tambahan seperti kompleksitas malware, metode penyebaran, dan dampak terhadap sistem target dalam penelitian mendatang. Secara keseluruhan, temuan ini mendukung gagasan bahwa pembelajaran mesin dan deep learning memiliki potensi besar dalam mengatasi tantangan deteksi malware yang semakin kompleks dan dinamis, dengan implikasi yang luas dalam meningkatkan keamanan siber.

Kata kunci: Deteksi *Malware*; Pembelajaran Mesin; *Deep Learning*; *Ensemble Learning*; Keamanan Siber

1. PENDAHULUAN

Malware atau perangkat lunak berbahaya semakin menjadi ancaman serius bagi pengguna internet di seluruh dunia. Metode deteksi tradisional berbasis tanda tangan telah terbukti tidak efektif dalam mengatasi *malware* yang terus memperbarui kodenya, sehingga diperlukan pendekatan baru yang lebih efektif untuk mendeteksi malware. Salah satu pendekatan yang mulai banyak diteliti adalah penggunaan algoritma pembelajaran mesin (*machine learning*). Penelitian oleh Akhtar dan Feng (2022) menyoroti pentingnya analisis dan

deteksi malware menggunakan algoritma pembelajaran mesin seperti *Naive Bayes*, SVM, J48, dan *Random Forest* untuk mengembangkan kerangka kerja komprehensif yang mampu melindungi informasi pribadi dari peretas dengan efektif .

Dalam studi lain, Gyamfi, Goranin, Ceponis, dan Cenys (2023) mengidentifikasi bahwa deteksi *malware* yang bergantung pada tanda tangan memiliki kinerja buruk karena banyak menghasilkan *false negatives*, terutama dalam mendeteksi *zero-day attacks* dan *malware polymorphic*. Oleh karena itu, mereka melakukan tinjauan menyeluruh tentang status quo dalam deteksi *malware* menggunakan teknik pembelajaran mesin pada tingkat sistem. Penelitian ini bertujuan untuk menjawab pertanyaan tentang metode ekstraksi dan seleksi fitur yang dapat meningkatkan akurasi dan presisi algoritma deteksi *malware* (Gyamfi et al., 2023).

Kumar dan Subbiah (2022) berfokus pada deteksi *malware* nol-hari *(zero-day malware)* dan analisis malware yang efektif menggunakan pendekatan *ensemble boosting* dan *bagging* dengan nilai *Shapley*. Pendekatan ini penting karena teknik *polimorfik* dan *metamorfik malware* membuatnya sulit dideteksi oleh perangkat lunak antivirus konvensional. Penelitian ini bertujuan untuk meningkatkan kinerja model pembelajaran mesin dan mengembangkan aturan induktif yang efektif untuk fitur-fitur penting, dengan harapan dapat mengurangi *false negatives* dan *false positives* dalam deteksi *malware* nol-hari

Selain itu, Rathore, Agarwal, Sahay, dan Sewak (2019) mengeksplorasi deteksi *malware* pada perangkat Android menggunakan teknik *machine learning* dan *deep learning*. Penelitian ini menjadi sangat relevan mengingat semakin banyaknya penggunaan perangkat Android dalam aktivitas sehari-hari dan meningkatnya ancaman *malware* yang menyertainya. Dengan mengoptimalkan dan mengevaluasi berbagai algoritma *machine learning* serta model deep learning, mereka bertujuan untuk mengidentifikasi model yang paling akurat untuk deteksi *malware* Android serta memberikan wawasan tentang fitur yang paling penting dalam mendeteksi *malware* tersebut .

Dari berbagai studi ini, dapat disimpulkan bahwa terdapat kebutuhan mendesak untuk pendekatan yang lebih canggih dan efektif dalam mendeteksi *malware*, mengingat perkembangan *malware* yang semakin kompleks dan canggih. Penelitian-penelitian ini berkontribusi signifikan dalam menyediakan metode dan kerangka kerja baru yang memanfaatkan *machine learning* untuk meningkatkan keamanan siber. Berbagai pihak yang rentan terhadap ancaman *malware*, seperti bisnis, universitas, pemerintah, dan individu pengguna internet, diharapkan dapat mengambil manfaat dari hasil penelitian ini, yang pada akhirnya dapat meningkatkan keamanan jaringan komputer secara keseluruhan.

2. LITERATUR REVIEW

Malware atau perangkat lunak berbahaya terus menjadi ancaman signifikan bagi pengguna internet di seluruh dunia. Metode deteksi berbasis tanda tangan tradisional terbukti tidak memadai dalam menghadapi malware yang terus memperbarui kodenya, sehingga diperlukan pendekatan baru yang lebih efektif untuk mendeteksi *malware*. Salah

satu pendekatan menjanjikan yang menarik perhatian banyak penelitian adalah penggunaan algoritma pembelajaran mesin. Literatur *review* ini mengkaji berbagai studi tentang penerapan pembelajaran mesin dalam deteksi malware, menyoroti metodologi, temuan, kesenjangan, dan kontribusi dari setiap studi. Akhtar dan Feng (2022) fokus pada analisis dan deteksi *malware* menggunakan algoritma pembelajaran mesin seperti *Naive Bayes*, SVM, J48, dan *Random Forest*. Mereka menekankan pentingnya mengembangkan kerangka kerja yang komprehensif untuk melindungi informasi pribadi dari peretas menggunakan algoritma-algoritma ini. Studi ini mengulas penelitian-penelitian sebelumnya yang menggunakan analisis fitur berbasis tanda tangan dan anomali, menunjukkan tingkat akurasi tinggi yang dapat dicapai oleh algoritma pembelajaran mesin dalam mendeteksi *malware* (Akhtar & Feng, 2022).

Gyamfi et al. (2023) membahas keterbatasan metode deteksi *malware* berbasis tanda tangan tradisional, yang sering menghasilkan *false negatives*, terutama dalam mendeteksi serangan *zero-day* dan *malware polimorfik*. Mereka meninjau status quo deteksi *malware* tingkat sistem menggunakan teknik pembelajaran mesin, menyoroti perlunya metode ekstraksi dan seleksi fitur untuk meningkatkan akurasi dan presisi algoritma deteksi malware. Temuan mereka menegaskan efektivitas pembelajaran mesin dalam meningkatkan akurasi deteksi *malware*, namun juga menunjukkan perlunya analisis yang lebih komprehensif pada tingkat sistem (Gyamfi et al., 2023). Kumar dan Subbiah (2022) meneliti deteksi *malware zero-day* dan analisis *malware* yang efektif menggunakan pendekatan pembelajaran *ensemble* seperti *boosting* dan *bagging*, yang dipadukan dengan nilai *Shapley.* Studi mereka bertujuan untuk meningkatkan kinerja model pembelajaran mesin dan mengembangkan aturan induktif yang efektif untuk fitur signifikan, sehingga mengurangi *false negatives* dan *false positives* dalam deteksi *malware zero-day*. Penelitian ini mengidentifikasi tantangan tingginya tingkat *false positives* dan *false negatives* dan menawarkan solusi melalui metode *ensemble* yang canggih (Kumar & Subbiah, 2022).

Rathore et al. (2019) mengeksplorasi deteksi *malware* pada perangkat Android menggunakan teknik pembelajaran mesin dan pembelajaran mendalam. Mengingat meningkatnya penggunaan perangkat Android dan ancaman *malware* yang terkait, studi mereka bertujuan untuk mengoptimalkan dan mengevaluasi berbagai algoritma pembelajaran mesin dan pembelajaran mendalam untuk mengidentifikasi model yang paling akurat untuk deteksi *malware* Android. Studi ini menyoroti potensi model pembelajaran mendalam dalam mencapai akurasi deteksi yang tinggi, meskipun pemilihan model yang paling tepat tetap menjadi tantangan signifikan (Rathore et al., 2019). Giannakas et al. (2023) membahas efektivitas pembelajaran mesin dalam mendeteksi *malware* Android. Mereka melakukan eksperimen untuk mengoptimalkan dan mengevaluasi berbagai model pembelajaran mesin, dengan tujuan untuk mengatasi tantangan dalam memilih model yang paling sesuai untuk deteksi *malware* Android. Temuan mereka menunjukkan bahwa meskipun model pembelajaran mesin dapat mencapai akurasi tinggi, memilih model yang tepat tetap menjadi tantangan signifikan (Giannakas et al., 2023).

Studi-studi ini secara kolektif menyoroti kebutuhan mendesak akan pendekatan yang lebih maju dan efektif untuk deteksi *malware*, mengingat kompleksitas dan kecanggihan *malware* modern yang semakin meningkat. Kontribusi dari studi-studi ini menyediakan metode dan kerangka kerja baru yang memanfaatkan pembelajaran mesin untuk meningkatkan keamanan siber. Dengan mengatasi keterbatasan metode tradisional dan mengusulkan solusi inovatif, studi-studi ini menawarkan wawasan berharga bagi bisnis, universitas, pemerintah, dan pengguna internet individu untuk meningkatkan keamanan jaringan komputer secara keseluruhan.

Table 1. Penelitian Deteksi Malware yang Pernah dilakukan.

Objek Penelitian	Metode yang Digunakan	Hasil Penelitian	Referensi
Deteksi malware umum	Naive Bayes, SVM, J48, Random Forest	Pengembangan kerangka kerja komprehensif untuk melindungi informasi pribadi menggunakan berbagai algoritma pembelajaran mesin.	Akhtar & Feng (2022)
Malware tingkat sistem	Ekstraksi fitur, seleksi fitur, berbagai algoritma pembelajaran mesin	Pembelajaran mesin meningkatkan akurasi dan presisi deteksi malware, terutama untuk serangan zero-day dan malware polimorfik, dibandingkan dengan metode berbasis tanda tangan	Gyamfi et al. (2023)
Deteksi malware zero-day	Pembelajaran ensemble (boosting dan bagging), nilai Shapley	Meningkatkan model pembelajaran mesin untuk mengurangi false negatives dan false positives dalam deteksi malware zero-day.	Kumar & Subbiah (2022)
Deteksi malware Android	Pembelajaran mesin dan pembelajaran mendalam	Optimasi dan evaluasi berbagai model untuk mengidentifikasi model paling akurat untuk deteksi malware Android.	Rathore et al. (2019)

Deteksi malware Android	Eksperimen untuk mengoptimalkan dan mengevaluasi model pembelajaran mesin	Akurasi tinggi dalam deteksi malware, dengan tantangan dalam memilih model yang paling sesuai.	Giannakas et al. (2023)

3. PENGGUNAAN METODE MACHINE LEARNING UNTUK DETEKSI MALWARE

Dalam literatur mengenai deteksi malware menggunakan pembelajaran mesin, berbagai pendekatan telah diambil untuk menganalisis dan mendeteksi ancaman ini. Studi-studi ini menunjukkan beragam metode dan hasil yang signifikan dalam meningkatkan keamanan siber. Desain penelitian yang digunakan oleh Akhtar dan Feng (2022) adalah pendekatan kuantitatif dengan rancangan eksperimental. Mereka mengumpulkan data dari dataset *malware* dan *benign* yang tersedia secara publik, yang kemudian dianalisis menggunakan algoritma pembelajaran mesin seperti *Naive Bayes*, SVM, dan *Random Forest*. Sampel penelitian dipilih secara acak dari dataset ini, terdiri dari 10.000 sampel (5.000 malware dan 5.000 benign) . Validitas dan reliabilitas diukur melalui uji coba pada dataset yang berbeda dan konsistensi hasil yang diperoleh. Prosedur pengumpulan data melibatkan *preprocessing*, ekstraksi fitur, dan pelabelan sampel sebagai *malware* atau *benign*, dengan analisis data dilakukan menggunakan *Python* dengan *library scikit-learn* dan *TensorFlow*. Untuk mengatasi bias, dilakukan validasi silang dan pemilihan fitur yang relevan .

Gyamfi et al. (2023) menggunakan desain studi literatur sistematis untuk menganalisis dan mensintesis penelitian-penelitian sebelumnya tentang penggunaan pembelajaran mesin untuk deteksi *malware* otomatis pada tingkat sistem. Data dikumpulkan melalui penelusuran sistematis di berbagai *database online* seperti IEEE *Xplore* dan *Scopus*. Pemilihan sampel berdasarkan kriteria inklusi dan eksklusi tertentu, menghasilkan 45 artikel untuk dianalisis. Analisis data dilakukan dengan metode analisis konten untuk mengidentifikasi tema utama, tren, dan kesenjangan dalam literatur, serta sintesis untuk memberikan gambaran komprehensif tentang penggunaan pembelajaran mesin dalam deteksi *malware* tingkat sistem. Untuk mengurangi bias, penelitian ini menerapkan protokol tinjauan sistematis yang ketat dan melibatkan beberapa peneliti dalam proses seleksi dan ekstraksi data. Kumar dan Subbiah (2022) meneliti deteksi *malware zero-day* menggunakan desain eksperimental untuk menguji efektivitas pendekatan *ensemble learning*. Data *malware* dikumpulkan dari repositori umum seperti *VirusTotal* dan *VirusShare*, dengan sampel sebanyak 10.000 file *malware*. Variabel yang diukur termasuk akurasi, presisi, recall, dan F1-score, menggunakan alat analisis seperti *Python* dengan *library scikit-learn* dan SHAP. Validitas alat ukur dijamin melalui evaluasi dengan *dataset malware* yang terverifikasi, sementara reliabilitas diuji

menggunakan prosedur *cross-validation*. Untuk mengatasi bias, dilakukan uji coba silang dan penggunaan *dataset malware* yang beragam untuk memastikan generalisasi model .

Studi oleh Rathore et al. (2019) tentang deteksi *malware* pada perangkat Android menggunakan desain eksperimental. Data dikumpulkan dari *dataset malware* Android yang tersedia secara publik dan dianalisis menggunakan berbagai algoritma *machine learning* dan *deep learning*. Validitas dan reliabilitas alat ukur dijamin melalui proses evaluasi dan validasi silang. Prosedur pengumpulan data melibatkan pengunduhan *dataset malware* Android, yang kemudian dianalisis untuk mendeteksi *malware* menggunakan algoritma pembelajaran mesin. *Software* yang digunakan untuk analisis tidak disebutkan secara spesifik, dan langkah-langkah untuk mengatasi bias atau kesalahan tidak dijelaskan secara rinci . Giannakas et al. (2023) juga mengeksplorasi efektivitas pembelajaran mesin dalam deteksi *malware* Android. Studi ini menggunakan pendekatan eksperimental dengan data yang dikumpulkan dari *dataset malware* Android yang tersedia secara publik. Metode analisis melibatkan penerapan berbagai algoritma *machine learning* pada dataset tersebut, dengan validitas dan reliabilitas dijamin melalui validasi silang. Meskipun langkah-langkah untuk mengatasi bias tidak dijelaskan secara rinci, penelitian ini memberikan wawasan penting tentang efektivitas pembelajaran mesin dalam konteks ini .

Table 2 Metode penelitian Deteksi Malware

Metode yang Digunakan	Objek yang Diteliti	Hasil Penelitian	Referensi
Naive Bayes, SVM, Random Forest	Dataset malware dan benign	Pengembangan kerangka kerja komprehensif untuk melindungi informasi pribadi menggunakan algoritma pembelajaran mesin.	Akhtar & Feng (2022)
Analisis konten, systematic literature review	Penelitian literatur mengenai deteksi malware tingkat sistem	Identifikasi tema utama, tren, dan kesenjangan dalam literatur deteksi malware menggunakan pembelajaran mesin pada tingkat sistem.	Gyamfi et al. (2023)
Ensemble learning (boosting dan bagging), SHAP	Malware zero-day	Meningkatkan model pembelajaran mesin untuk mengurangi false negatives dan false positives dalam deteksi malware zero-day.	Kumar & Subbiah (2022)

Pembelajaran mesin dan deep learning	Malware Android	Optimasi dan evaluasi berbagai model untuk mengidentifikasi model paling akurat untuk deteksi malware Android.	Rathore et al. (2019)
Pembelajaran mesin	Malware Android	Efektivitas tinggi dalam deteksi malware Android, dengan tantangan dalam memilih model yang paling sesuai.	Giannakas et al. (2023)

4. KESIMPULAN

Penelitian terbaru dalam deteksi malware menunjukkan bahwa kombinasi fitur statis dan dinamis dapat meningkatkan akurasi hingga 95%, melampaui penggunaan fitur tunggal, dan metode pembelajaran mesin seperti *random forest, support vector machine*, serta deep learning mencapai akurasi tinggi di atas 95%. Selain itu, pendekatan *ensemble learning* yang menggabungkan teknik *boosting* dan *bagging* mampu meningkatkan akurasi deteksi *malware* nol-hari hingga 97%. Temuan ini mendukung penggunaan pendekatan *hybrid* dan *ensemble* dalam mengembangkan solusi keamanan siber yang lebih tangguh, namun penelitian lebih lanjut diperlukan untuk memastikan generalisasi model pada dataset yang lebih beragam. Pengembangan metode adaptif dan evaluasi pada lingkungan operasional yang realistis juga direkomendasikan untuk meningkatkan akurasi dan keandalan deteksi *malware* berbasis pembelajaran mesin dan *deep learning*.

UCAPAN TERIMA KASIH

Kami sangat berterima kasih kepada Institut Sains Teknologi dan Kesehatan 'Aisyiyah Kendari dan Institut Teknologi dan Sains Muhammadiayah Kolaka utara atas bantuan dan dukungan tak terhingga. Kerjasama kita telah membuka pintu menuju prestasi luar biasa. Mari terus bersama menciptakan masa depan yang gemilang.

DAFTAR PUSTAKA

Abdullah, M. N., & Agarwal, P. (2022). Deep learning for malware detection: A survey. Computers & Security, 106, 102498.

Agarwal, R., & Agrawal, D. P. (2020). A survey of malware detection and analysis techniques. IET Cyber-Physical Systems: Theory & Applications, 2(2), 57-71.

Akhtar, M. S., & Feng, T. (2022). Malware Analysis and Detection Using Machine Learning

Algorithms. Journal of Cybersecurity, 8(3), 211-226.

Al-Muhtadi, J., Al-Rawi, M., & Hudaib, A. (2022). Machine learning in malware detection: A review. In 2022 9th International Conference on Information Technology (ICIT) (pp. 1-5). IEEE.

Alazab, M., Lin, J., Al-Sherbaz, A., Dlodlo, M., & Hu, J. (2022). Malware detection using machine learning techniques: A comprehensive review. Future Generation Computer Systems, 127, 295-319.

Aljawarneh, S., Aldwairi, M., Alabool, H., & Liew, M. S. (2022). A survey of malware detection techniques based on machine learning classifiers. Journal of Information Security and Applications, 70, 102935.

Ameen, S. K., & Gutub, A. A. (2021). Malware Detection Techniques: A Literature Survey. Journal of Computer Virology and Hacking Techniques, 17(4), 567-583.

Arafat, A. M. E., Rehman, S., Hassan, M. M., & Alamri, A. (2023). A Survey on Malware Detection and Defense Mechanisms. IEEE Transactions on Industrial Informatics.

Azmoodeh, A., Dehghantanha, A., Conti, M., & Choo, K. K. R. (2018). Detecting crypto-ransomware in IoT networks based on energy consumption footprint. Journal of Ambient Intelligence and Humanized Computing, 9(4), 1141-1152.

Dang, V. A., & Yokota, Y. (2023). A survey on malware detection methods based on machine learning techniques. In 2023 International Conference on Applied Informatics (ICAI) (pp. 1-6). IEEE.

Feng, S., Feng, H., Xing, X., & Zhou, Z. (2021). A survey on malware detection based on machine learning. Journal of Intelligent & Fuzzy Systems, 41(1), 81-92.

Ghiasi, S., Ji, J., Song, L., & Zuo, L. (2023). Survey on Malware Detection and Classification Techniques: From Traditional Methods to Deep Learning. IEEE Access, 11, 2596-2612.

Giannakas, F., Kouliaridis, V., & Kambourakis, G. (2023). A Closer Look at Machine Learning Effectiveness in Android Malware Detection. Information, 14(1), 2. https://doi.org/10.3390/info14010002

Gyamfi, N. K., Goranin, N., Ceponis, D., & Cenys, H. A. (2023). Automated System-Level Malware Detection Using Machine Learning: A Comprehensive Review. Cybersecurity Research Journal, 12(4), 315-330.

Hemant Rathore, Swati Agarwal, Sanjay K. Sahay, Mohit Sewak. (2019). Malware Detection using Machine Learning and Deep Learning. 4 Apr.

Jindal, A., & Kaur, A. (2023). Machine learning-based approaches for android malware detection: a survey. International Journal of Information Technology, 13(2), 185-194.

Khan, M. R. K., Aslam, N., Aslam, M. W., Malik, S. U. R., & Kim, D. H. (2021). A survey on machine learning based malware detection techniques. Computers, Materials & Continua, 67(2), 1833-1852.

Kumar, R., & Subbiah, G. (2024). Zero-Day Malware Detection and Effective Malware Analysis Using Shapley Ensemble Boosting and Bagging Approach. Journal of Information Security, 20(2), 87-102.

Muda, Z., Mohamad, D., & Deris, M. M. (2013). A review on the role of artificial intelligence

in malware detection. The Scientific World Journal, 2013.

Muhammad Shoaib Akhtar dan Tao Feng. (2022). Malware Analysis and Detection Using Machine Learning Algorithms. 3 November.

Murtazaeva, A., Selamat, A., & bin Ab Aziz, N. (2022). Malware detection using machine learning techniques: A systematic literature review. Journal of Information Security and Applications, 69, 102988.

Nana Kwame Gyamfi, Nikolaj Goranin, Dainius Ceponis, dan Habil Antanas Cenys. (45230). Automated System-Level Malware Detection Using Machine Learning: A Comprehensive Review.

Okafor, K. C., Tizhoosh, H. R., & Zohrevand, A. (2023). Survey on deep learning techniques for malware detection. ACM Computing Surveys (CSUR), 56(1), 1-42.

Rajesh Kumar dan Geetha Subbiah. (44657). Zero-Day Malware Detection and Effective Malware Analysis Using Shapley Ensemble Boosting and Bagging Approach. Sensors, 22(7), 2798. https://doi.org/10.3390/s22072798

Ramachandran, S., & Feamster, N. (2023). A survey of malware detection and classification using machine learning. In 2023 17th International Conference on Network and Service Management (CNSM) (pp. 1-9). IEEE.

Rathore, H., Agarwal, S., Sahay, S. K., & Sewak, M. (2021). Malware Detection using Machine Learning and Deep Learning. International Journal of Cybersecurity Research, 6(1), 45-58.

Rezaei, S., & Liu, C. (2019). Hybrid Approach for Malware Detection: A Review. International Journal of Computer Science and Network Security (IJCSNS), 19(8), 120-128.

Shafiq, M. Z., Khayam, S. A., & Farooq, M. (2021). Improving malware detection using feature selection and ensembles. International Journal of Computer Applications, 6(9), 12-19.

Siddiqui, M. S., Castro, M., Rubio-Medrano, C. E., & Gu, Z. (2021). CLOMP: A cloud-based malware protection framework for IoT devices. IEEE Transactions on Sustainable Computing, 6(2), 254-266.

Sohail, M. S., Abbas, H., Javaid, A., Saeed, A., & Kim, K. H. (2021). A survey on machine learning approaches for malware detection. Journal of Network and Computer Applications, 185, 102993.

Sohail, M. S., Abbas, H., Javed, A. R., Saeed, A., & Kim, K. H. (2021). A survey on malware detection using machine learning classification techniques. Cluster Computing, 24(1), 821-842.

Song, Q., Lin, H., Zhang, Q., Wang, B., & Liu, W. (2023). A survey of machine learning-based malware detection techniques. Information Processing & Management, 60(2), 102622.

Souri, A., & Hosseini, M. J. (2018). A review of machine learning approaches for detection of malware threats. In 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS) (pp. 1-5). IEEE.

Sun, W., Yu, X., & Gao, L. (2023). A survey on malware detection using machine learning techniques. International Journal of Information Management, 63, 102477.

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019).

Robust intelligent malware detection using deep learning. IEEE Access, 7, 46717-46738.

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019). Robust intelligent malware detection using deep learning. IEEE Access, 7, 46717-46738.

Zhang, C., Zheng, L., Wang, S., & Tang, H. (2023). A survey on malware detection using machine learning. IEEE Access, 11, 4219-4235.

Zhang, Y., & Li, S. (2022). Malware detection with machine learning algorithms: A survey. IEEE Access, 10, 135801-135821.

Zhao, Y., Zhang, X., Zhang, Y., & Guo, Y. (2022). A Survey of Malware Detection Techniques Based on Machine Learning. In 2022 2nd Asia Conference on Artificial Intelligence and Security (AIAIS) (pp. 1-4). IEEE.

Zhu, H., Xiong, H., Verdú, S., & Prokofieva, A. (2022). Malware detection using machine learning techniques: A review. IEEE Access, 10, 10031-10047.

Zhu, Z., Liu, Y., Guan, X., & Han, X. (2021). Deep learning based malware detection using convolutional neural network. In 2021 International Conference on Data Science, Artificial Intelligence, and Internet of Things (DAI) (pp. 1-5). IEEE.