PENERAPAN METODE *RT-AMD* DALAM ANALISIS DETEKSI SERANGAN *MALWARE* PADA LINGKUNGAN *CLOUD COMPUTING*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

SITI TRIWINARTI NINGRUM

09011382025145

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

PENERAPAN METODE *RT-AMD* DALAM ANALISIS DETEKSI SERANGAN *MALWARE* PADA LINGKUNGAN *CLOUD COMPUTING*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

SITI TRIWINARTI NINGRUM
09011382025145

Palembang, 17 Januari 2025

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. Sukemi, M.T.	**Dr. Ir. Ahmad Heryanto, S. Kom, M.T**
NIP. 196612032006041001	NIP. 198701222015041002

AUTHENTICATION PAGE

THE APPLICATION OF THE RT-AMD METHOD IN ANALYZING MALWARE ATTACK DETECTION IN CLOUD COMPUTING ENVIRONMENT

THESIS

Dept. of Computer System

Bachelor's Degree

By:

Siti Triwinarti Ningrum

09011382025145

Palembang, 9 Januari 2025

Head Of Computer System Department	*Supervisor*
Dr. Ir. Sukemi, M.T.	**Dr. Ir. Ahmad Heryanto, S. Kom, M.T**
NIP. 196612032006041001	**NIP. 198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Senin

Tanggal : 23 Desember 2024

Tim Penguji :

1. Ketua : Aditya Putra Perdana Prasetyo, S.Kom., M.T _____

2. Penguji : Huda Ubaya, S.T., M.T. _____

3. Pembimbing : Dr. Ahmad Heryanto, S.Kom., M.T _____

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr.Ir. Sukemi, M.T.
NIP.19661203200604001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Siti Triwinarti Ningrum
NIM : 09011382025145
Judul : Penerapan Metode *RT-AMD* Dalam Analisis Deteksi Serangan *Malware* Pada Lingkungan *Cloud computing*.

Hasil Pengecekan Software iThenticate/Turnitin: 3%

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

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

Indralaya, 10 Januari 2025

Siti Triwinarti Ningrum
NIM.09011382025145

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Segala Puji dan Syukur penulis Panjatkan ke hadirat Allah SWT yang telah melimpahkan berkah, rahmat dan karunia-Nya sehingga penulis dapat menyusun dan menyelesaikan skripsi ini yang berjudul "Penerapan Metode *RT-AMD* Dalam Analisis Deteksi Serangan *Malware* Pada Lingkungan *Cloud computing*" ini dengan baik dan lancar.

Selesainya penulisan skripsi ini tidak lepas dari berbagai pihak yang telah membimbing serta membantu. Oleh karena itu, dengan penuh rasa hormat dan tulus, penulis ingin menyampaikan rasa syukur yang mendalam serta ucapan terima kasih kepada:

1. Allah SWT yang telah memberikan Berkah dan Rahmatnya agar penulis dapat menyelesaikan penulisan skripsi ini dengan baik dan lancar.
2. Mama dan Papa penulis atas segala doa yang tiada henti , dukungan dan kasih sayang yang selalu diberikan kepada penulis sehingga penulis dapat menyelesaikan penulisan skripsi ini dengan penuh semangat.
3. Kedua kakak penulis, yang selalu memotivasi dan memberikan bimbingan berharga, baik dalam perjalanan akademik maupun kehidupan pribadi kepada penulis.
4. Keluarga Besar penulis atas doa dan dukungan moral kepada penulis.
5. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
6. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
7. Bapak Dr. Ahmad Heryanto, S. Kom, M.T selaku Dosen Pembimbing Tugas Akhir, atas bimbingan, dukungan dan arahan yang sangat berharga selama penyusunan Tugas Akhir ini.
8. Bapak Rossi Passarella, S.T., M.Eng., selaku Dosen Pembimbing Akademik.

9. Mba Sari Nuzulastri, selaku Admin Jurusan Sistem Komputer Bukit.
10. Sahara Diva Maharani, Ully Afifa, M.Aziz Alhadi, Ghulam Robbani Toha, Luqman Agus Dwiyono selaku teman yang senantiasa menemani hari-hari penulis selama proses penulisan skripsi ini, serta turut membantu dan memberikan dukungan moral yang berarti.
11. Hanif Azfa Sadifatiasmi dan Bayu Akbar Pebrian selaku teman yang selalu membantu sejak awal perkuliahan hingga saat ini dan selalu memberikan arahan serta dukungan kepada penulis .
12. Sahabat – sahabat tercinta, Tiara, Nyayu, Ardel yang selalu mendampingi, memberikan dukungan, serta semangat tanpa henti sepanjang perjalanan penulisan skripsi ini.
13. Grup APSI dan Crack Illegal yang selalu kompak.
14. Semua pihak yang telah membantu yang tidak dapat saya sebutkan satu persatu.

Penulis menyadari bahwa kesempurnaan hanyalah milik Allah SWT, sehingga kritik, saran dan masukan dari berbagai pihak yang berkenan sangat diharapkan untuk perbaikan di waktu yang akan datang.

Wassalamualaikum Warahmatullahi Wabarakatuh.

Palembang, Januari 2025
Penulis,

Siti Triwinarti Ningrum
NIM.09011382025145

PENERAPAN METODE *RT-AMD* DALAM ANALISIS DETEKSI SERANGAN *MALWARE* PADA LINGKUNGAN *CLOUD COMPUTING*

Siti Triwinarti Ningrum (09011382025145)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : sititriwinarti2166@gmail.com

ABSTRAK

Keamanan *cloud computing* menjadi isu penting seiring meningkatnya ancaman *malware* seperti *spyware, ransomware,* dan *trojan horse*. Penelitian ini mengembangkan sistem deteksi *malware* berbasis *RT-AMD (Real-Time Attack Monitoring and Detection)* menggunakan algoritma *Random Forest, Decision Tree, K-Nearest Neighbor,* dan *Naïve Bayes*. Dataset *CIC-MalMem-2022* digunakan sebagai basis analisis *multiclass* dengan kategori *benign, spyware, ransomware,* dan *trojan horse*. Tahapan meliputi *preprocessing*, penerapan SMOTE untuk menyeimbangkan data, seleksi fitur dengan *Correlation-Based Feature Selection* (CFS), dan evaluasi menggunakan akurasi, presisi, recall, F1-score, serta AUC. Dari hasil penelitian, algoritma *Random Forest* memberikan performa tertinggi dengan akurasi mencapai 83.97%, menunjukkan keandalannya dalam mendeteksi pola serangan *malware* secara efektif. Metode ini terbukti unggul dibandingkan algoritma lainnya dalam menangani klasifikasi multiclass pada dataset CIC-MalMem-2022. Penelitian ini memberikan kontribusi signifikan dalam pengembangan sistem deteksi *malware* yang lebih efektif, khususnya di lingkungan *cloud computing*, dan membuka peluang pengembangan lebih lanjut untuk menghadapi ancaman *siber* yang terus berkembang.

Kata Kunci : *Malware* Detection, RT-AMD, *Machine learning*, *Cloud computing*

THE APPLICATION OF THE RT-AMD METHOD IN ANALYZING MALWARE ATTACK DETECTION IN CLOUD COMPUTING ENVIRONMENT

Siti Triwinarti Ningrum (09011382025145)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : sititriwinarti2166@gmail.com

ABSTRACT

The security of cloud computing has become a critical issue with the rise of malware threats such as spyware, ransomware, and trojan horses. This study develops a malware detection system based on RT-AMD (Real-Time Attack Monitoring and Detection) using machine learning algorithms, including Random Forest, Decision Tree, K-Nearest Neighbor, and Naïve Bayes. The CIC-MalMem-2022 dataset is used as the basis for multiclass analysis, categorizing data into benign, spyware, ransomware, and trojan horse. The research stages include preprocessing, applying SMOTE to balance the data, feature selection with Correlation-Based Feature Selection (CFS), and evaluation using accuracy, precision, recall, F1-score, and AUC. The results show that the Random Forest algorithm achieves the highest performance with an accuracy of 83.97%, demonstrating its reliability in effectively detecting malware attack patterns. This method outperforms other algorithms in handling multiclass classification on the CIC-MalMem-2022 dataset. This study provides significant contributions to developing more effective malware detection systems, particularly in cloud computing environments, and opens opportunities for further advancements to address evolving cyber threats.

Key Words : *Malware Detection, RT-AMD, Machine learning, Cloud computing*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Malware atau perangkat lunak berbahaya, merupakan perangkat lunak yang dirancang khusus untuk mengganggu, merusak, atau mengakses sistem atau jaringan komputer secara tidak sah. Berdasarkan tujuan dan cara penyebarannya, *malware* dapat dibagi ke dalam beberapa kategori yang dapat saling bersinggungan [1]. Adapun kategori *malware* meliputi, *adware*, *backdoor*, *ransomware*, *rookit*, *spyware*, *trojan*, *virus*, *warm* dan *botnet*.

Cloud computing juga juga rentan terhadap serangan *malware*, *Cloud computing* merupakan salah satu pendorong utama produktivitas yang menawarkan cara nyaman untuk memperoleh kualitas tinggi aplikasi dengan layanan hosting, pengiriman, dan penyimpanan melalui Internet. Teknologi *Cloud computing* menggunakan infrastruktur internet untuk mengakses dan memanfaatkan sumber daya dalam pengelolaan, pemrosesan, dan penerapan data [2].

Namun perlu diketahui bahwa penelitian mengenai analisis deteksi serangan *malware* di lingkungan *cloud* sudah banyak dibahas seperti pada penelitian [3] yang membahas mengenai pengembangan sistem deteksi *malware* cerdas dalam lingkungan *Cloud computing*. Dalam sistem yang diusulkan, data *malware* dari berbagai sumber dikumpulkan dan fitur-fitur yang spesifik diidentifikasi secara efisien. Fitur-fitur tersebut kemudian digunakan oleh agen pendeteksi berbasis *machine learning* (ML) dan aturan untuk membedakan *malware* dari sampel yang tidak berbahaya. Evaluasi kinerja sistem yang diusulkan dilakukan dengan menganalisis 10.000 sampel program, yang menunjukkan kemampuan sistem dalam mendeteksi baik *malware* yang dikenal maupun tidak dikenal dengan tingkat deteksi dan akurasi yang tinggi. Algoritme yang diusulkan bersama dengan pengklasifikasi pembelajaran mesin mencapai tingkat deteksi sebesar 99,8%, tingkat positif palsu sebesar 0,4%, dan akurasi sebesar 99,7%. Hasil penelitian ini dapat memberikan kontribusi bagi pengembangan sistem deteksi *malware* baru di lingkungan *cloud*.

Lalu penelitian [4] memaparkan mengenai metode pendektesian *malware* berbasis perilaku online yang menggunakan dua jenis *Recurrent Neural Network* (RNN) untuk insfrastruktur cloud. Metode ini bekerja dengan memonitor perilaku *virtual machine* (VM) secara real-time, metode ini menggunakan LSTM dan GRU untuk mendeteksi anomali sebagai tanda keberadaan *malware*. Evaluasi terhadap keduanya menunjukkan arkurasi tinggi: LSTM mencapai 98,7%, sementara GRU mencapai 97,5%. Metode ini unggul dalam mendeteksi *malware zero-day* dan mengatasi upaya pengelabuan terhadap metode deteksi tradisional. Secara keseluruhan, pendekatan RNN menjanjikan untuk deteksi *malware* efektif di lingkungan cloud.

Kemudian penelitian [5] membahas mengenai pendekatan efisiensi untuk mendeteksi lalu lintas botnet dengan menggunakan teknik pemilihan fitur dan mengevaluasi tiga subset fitur dan tiga model yaitu algoritma *Decision Tree, Random Forest* dan *K-Nearest Neighbor*. Metodologi melibatkan pemilihan fitur yan relevan dari data jaringan menggunakan analisi korelasi dan pemilihan fitur, serta implementasi *Decision Tree* untuk membangun model deteksi. Pada penelitian ini menggunakan dataset CTU-13 yaitu QB-CTU13 dan EQB-CTU13, menunjukkan bahwa pemilihan fitur meningkatkan efisiensi dan akurasi model dibandingkan dengan menggunakan semua fitur. Hasil dari penelitian ini menunjukkan bahwa *Decision Tree* mencapai kinerja tertinggi dengan menggunakan set fitur lima, yang memperoleh F1-Score rata-rata 85% dengan waktu rata-rata 0,78 mikrodetik untuk mengklasifikasikan setiap sampel.

Pada penelitian [6] membahas mengenai penerapan *machine learning* dalam mengidentifikasi dan mencegah lalu lintas botnet. Penelitian ini menggunakan algoritma *Random Forest* (RF) dan *Decision Tree* (CART), menunjukkan bahwa manipulasi dataset, termasuk segmentasi lalu lintas dan penggunaan alamat IP serta port, dapat meningkatkan akurasi deteksi deteksi botenet meskipun menurunkan F1-Score. Hal ini dapat dijadikan dasar untuk mengembangkan model *machine learning* yang lebih efektif dalam melawan serangan botnet.

Pada penelitian [7] *RT-AMD* menggunakan berbagai algoritma klasifikasi, termasuk *Naïve Bayes, K-Nearest Neighbor (KNN), Decision Tree,* dan *Random*

Forest, untuk membangun model prediktif yang dapat mengidentifikasi lalu lintas jaringan mencurigakan yang mungkin menunjukkan serangan DDoS. Keunggulan utama *RT-AMD* adalah kemampuannya dalam mendeteksi serangan secara real-time, yang sangat penting untuk lingkungan *cloud* yang dinamis dan rentan terhadap serangan DDoS. Model ini telah diuji dengan dataset DDoS-2020, dan menunjukkan akurasi sangat tinggi, mencapai 99,38% dengan algoritma *Random Forest* di lingkungan *cloud*. Selain itu, akurasi serupa juga diperoleh saat menggunakan dataset *NSL-KDD.*

RT-AMD (Real-Time Attack Monitoring and Detection) merupakan pilihan yang menarik karena mengandalkan berbagai teknik *machine learning*, di mana banyak penelitian terdahulu telah membahas deteksi *malware* menggunakan model algoritma *machine learning*. Berdasarkan penjabaran tersebut, penelitian ini juga akan menerapkan metode *RT-AMD* dengan menggunakan algoritma *machine learning* seperti *Random Forest, Decision Tree, Naïve Bayes, dan K-Nearest Neighbors*. Penelitian ini akan menggunakan dataset *CIC-MalMem-2022*, yang mencakup berbagai jenis serangan siber, termasuk serangan *malware botnet*. Dengan demikian, penulis mengusulkan penelitian dengan judul "Penerapan Metode *RT-AMD* dalam Analisis Deteksi Serangan *Malware* Pada Lingkungan *Cloud computing*".

1.2 Perumusan Masalah

Berdasarkan pemaparan dari latar belakang diatas maka penulis menguraikan beberapa rumusan masalah dari penelitian ini , yaitu:

1. Bagaimana mempersiapkan dan memproses data dari dataset *CIC-MalMem-2022* untuk digunakan dalam model deteksi serangan *malware*?
2. Bagaimana efektivitas kinerja model *Decision Tree*, *Random Forest*, *K-Nearest Neighbor*, dan *Naïve Bayes* dalam dataset *CIC-MalMem-2022*?

1.3 Batasan Masalah

Agar pembahasan yang dilakukan lebih tearah dan tidak menyimpang dari permasalahan yang ada serta dibuat lebih terfokus , maka penulis memberikan batasan masalah sebagai berikut:

1. Dataset yang digunakan terbatas pada *CIC-MalMem-2022*, yang sudah mencakup berbagai jenis serangan dan data normal.
2. Jenis data serangan yaitu *Spyware, Ransomware, Trojan Horse.*
3. Penelitian ini membatasi model yang digunakan hanya algoritma *Decision Tree*, *Random Forest*, *K-Nearest Neighbor*, dan *Naïve Bayes.*
4. Penelitian ini hanya mempertimbangkan serangan dalam lingkungan *Cloud computing* yang berdasarkan pada dataset *CIC-MalMem-2022.*

1.4 Tujuan

Adapun tujuan dari penelitian ini sebagai berikut:

1. Mengidentifikasi fitur penting pada dataset *CIC-MalMem-2022* dan menerapkan teknik *SMOTE* untuk menyeimbangkan data dalam deteksi serangan *malware.*
2. Meningkatkan kinerja model *Decision Tree*, *Random Forest*, *K-Nearest Neighbor*, dan *Naïve Bayes* berdasarkan metrik evaluasi seperti akurasi, presisi, recall, dan F1-score.

1.5 Manfaat

Adapun manfaat dari penelitian ini sebagai berikut:

1. Dengan identifikasi fitur relevan dan penerapan SMOTE, model lebih efektif mengenali pola serangan, mengurangi bias, dan meningkatkan deteksi pada kelas minoritas, sehingga sistem deteksi *malware* menjadi lebih andal dan optimal.
2. Menganalisa hasil dari kinerja model *Decision Tree*, *Random Forest*, *K-Nearest Neighbor*, dan *Naïve Bayes* dalam pegujian pada dataset *CIC-MalMem-2022.*

1.6 Sistematika Penulisan

Dalam penyusunan tugas akhir, penulis akan mengikuti pendekatan sistematis dengan merinci setiap bab secara terurut. Setiap bab akan terdiri dari sejumlah sub-bab yang akan diuraikan secara rinci, menjelaskan dengan detail konten yang relevan. Secara sistematika, susunan penulisan dan penyusunan tugas akhir akan mengikuti struktur berikut:

BAB I. PENDAHULUAN

Bab ini membahas subbab-subbab seperti latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

BAB II . TINJAUAN PUSTAKA

Bab ini memaparkan penjelasan mengenai penelitian-penelitian terkait, hasil tinjauan literatur, landasan teori yang mendukung, serta ringkasan kajian pustaka yang relevan dengan topik penelitian.

BAB III. METODE PENELITIAN

Bab ini menguraikan metode penelitian yang mencakup proses pengumpulan dataset, spesifikasi perangkat keras maupun lunak yang digunakan, serta penjelasan tentang diagram blok dan metode yang diterapkan dalam penelitian.

BAB IV. ANALISIS DAN HASIL

Bab ini menguraikan analisis terhadap penelitian yang telah dilakukan serta memaparkan hasil yang diperoleh dari penelitian tersebut.

BAB V. PENUTUP

Bab ini mencakup kesimpulan dari penelitian yang telah dilakukan dan saran yang dapat diberikan untuk pengembangan penelitian di masa mendatang.

DAFTAR PUSTAKA

[1] D. Gibert, C. Mateu, and J. Planes, "The rise of *machine learning* for detection and classification of *malware*: Research developments, trends and challenges," *J. Netw. Comput. Appl.*, vol. 153, no. July 2019, p. 102526, 2020, doi: 10.1016/j.jnca.2019.102526.

[2] N. Eddermoug, A. Mansour, M. Azmi, M. Sadik, E. Sabir, and H. Bahassi, "A Literature Review on Attacks Prevention and Profiling in *Cloud computing*," *Procedia Comput. Sci.*, vol. 220, pp. 970–977, 2023, doi: 10.1016/j.procs.2023.03.134.

[3] O. Aslan, M. Ozkan-Okay, and D. Gupta, "Intelligent Behavior-Based *Malware* Detection System on *Cloud computing* Environment," *IEEE Access*, vol. 9, pp. 83252–83271, 2021, doi: 10.1109/ACCESS.2021.3087316.

[4] J. C. Kimmel, A. D. McDole, M. Abdelsalam, M. Gupta, and R. Sandhu, "Recurrent Neural Networks Based Online Behavioural *Malware* Detection Techniques for Cloud Infrastructure," *IEEE Access*, vol. 9, pp. 68066–68080, 2021, doi: 10.1109/ACCESS.2021.3077498.

[5] J. Velasco-Mata, V. Gonzalez-Castro, E. F. Fernandez, and E. Alegre, "Efficient Detection of Botnet Traffic by Features Selection and *Decision Trees*," *IEEE Access*, vol. 9, pp. 120567–120579, 2021, doi: 10.1109/ACCESS.2021.3108222.

[6] R. Abrantes, P. Mestre, and A. Cunha, "Exploring Dataset Manipulation via *Machine learning* for Botnet Traffic," *Procedia Computer Science*, vol. 196. pp. 133–141, 2021. doi: 10.1016/j.procs.2021.11.082.

[7] O. Bamasag, A. Alsaeedi, A. Munshi, D. Alghazzawi, S. Alshehri, and A. Jamjoom, "Real-time DDoS flood attack monitoring and detection (RT-AMD) model for *cloud computing*," *PeerJ Comput. Sci.*, vol. 7, pp. 1–21, 2022, doi: 10.7717/PEERJ-CS.814.

[8] P. Kotian and R. Sonkusare, "Detection of *Malware* in Cloud Environment using Deep Neural Network," *2021 6th Int. Conf. Converg. Technol. I2CT 2021*, pp. 21–25, 2021, doi: 10.1109/I2CT51068.2021.9417901.

[9] 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.

[10] M. Azeem, D. Khan, S. Iftikhar, S. Bawazeer, and M. Alzahrani, "Analyzing and comparing the effectiveness of *malware* detection: A study of *machine learning* approaches," *Heliyon*, vol. 10, no. 1, p. e23574, 2024, doi: 10.1016/j.heliyon.2023.e23574.

[11] K. S. Roy, T. Ahmed, P. B. Udas, M. E. Karim, and S. Majumdar, "MalHyStack: A hybrid stacked ensemble learning framework with feature

engineering schemes for obfuscated *malware* analysis," *Intelligent Systems with Applications*, vol. 20. 2023. doi: 10.1016/j.iswa.2023.200283.

[12] R. B. Hadiprakoso, H. Kabetta, and I. K. S. Buana, "Hybrid-Based *Malware* Analysis for Effective and Efficiency Android *Malware* Detection," *Proc. - 2nd Int. Conf. Informatics, Multimedia, Cyber, Inf. Syst. ICIMCIS 2020*, no. July 2021, pp. 8–12, 2020, doi: 10.1109/ICIMCIS51567.2020.9354315.

[13] 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.

[14] C. Okur and M. Dener, "Detecting IoT Botnet Attacks Using *Machine learning* Methods," *2020 Int. Conf. Inf. Secur. Cryptology, ISCTURKEY 2020 - Proc.*, pp. 31–37, 2020, doi: 10.1109/ISCTURKEY51113.2020.9307994.

[15] M. Aljabri *et al.*, "Ransomware detection based on *machine learning* using memory features," *Egypt. Informatics J.*, vol. 25, no. July 2023, p. 100445, 2024, doi: 10.1016/j.eij.2024.100445.

[16] G. Kale, G. E. Bostancı, and F. V. Çelebi, "Evolutionary feature selection for *machine learning* based *malware* classification," *Eng. Sci. Technol. an Int. J.*, vol. 56, no. February 2024, p. 101762, 2024, doi: 10.1016/j.jestch.2024.101762.

[17] N. Saran and N. Kesswani, "A comparative study of supervised *Machine learning* classifiers for Intrusion Detection in Internet of Things," *Procedia Comput. Sci.*, vol. 218, pp. 2049–2057, 2022, doi: 10.1016/j.procs.2023.01.181.

[18] B. M. Khammas, "Ransomware Detection using *Random Forest* Technique," *ICT Express*, vol. 6, no. 4, pp. 325–331, 2020, doi: 10.1016/j.icte.2020.11.001.

[19] 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.

[20] A. Alharbi and K. Alsubhi, "Botnet Detection Approach Using Graph-Based *Machine learning*," *IEEE Access*, vol. 9, pp. 99166–99180, 2021, doi: 10.1109/ACCESS.2021.3094183.

[21] 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 of Things and Cyber-Physical Systems*, vol. 3. pp. 100–111, 2023. doi: 10.1016/j.iotcps.2023.03.001.

[22] E. Odat, B. Alazzam, and Q. M. Yaseen, "Detecting *Malware* Families and Subfamilies using *Machine learning* Algorithms: An Empirical Study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 2, pp. 761–765, 2022, doi:

10.14569/IJACSA.2022.0130288.

[23] O. N. Elayan and A. M. Mustafa, "Android *malware* detection using deep learning," *Procedia Comput. Sci.*, vol. 184, no. 2019, pp. 847–852, 2021, doi: 10.1016/j.procs.2021.03.106.

[24] T. Zhukabayeva, "ScienceDirect ScienceDirect Enhancing Enhancing IoT IoT Security : Security : Effective Effective Botnet Botnet Attack Attack Detection Detection Through Through Machine *Machine learning* Learning," *Procedia Comput. Sci.*, vol. 241, pp. 421–426, 2024, doi: 10.1016/j.procs.2024.08.058.

[25] A. Hossain, T. Hasan, F. Ahmed, S. Hasib, M. Hasan, and A. Haque, "Cyber Security and Applications Towards superior android ransomware detection : An ensemble *machine learning* perspective," vol. 3, no. October 2024, 2025, doi: 10.1016/j.csa.2024.100076.

[26] W. N. H. Ibrahim *et al.*, "Multilayer Framework for Botnet Detection Using *Machine learning* Algorithms," *IEEE Access*, vol. 9, pp. 48753–48768, 2021, doi: 10.1109/ACCESS.2021.3060778.

[27] S. A. Bello *et al.*, "*Cloud computing* in construction industry: Use cases, benefits and challenges," *Autom. Constr.*, vol. 122, p. 103441, 2021, doi: 10.1016/j.autcon.2020.103441.

[28] P. H. B. Patel and P. N. Kansara, "*Cloud computing* Deployment Models: A Comparative Study," *Int. J. Innov. Res. Comput. Sci. Technol.*, vol. 9, no. 2, pp. 45–50, 2021, doi: 10.21276/ijircst.2021.9.2.8.

[29] R. Essah, "Investigating *Cloud computing* Security Measures and Risks International Journal of Research Publication and Reviews Investigating *Cloud computing* Security Measures and Risks .," no. February, 2024.

[30] S. Agarkar and S. Ghosh, "*Malware* detection & classification using *machine learning*," *Proc. - 2020 IEEE Int. Symp. Sustain. Energy, Signal Process. Cyber Secur. iSSSC 2020*, pp. 20–23, 2020, doi: 10.1109/iSSSC50941.2020.9358835.

[31] A. Yeboah-Ofori, "Classification of *Malware* Attacks Using *Machine learning* In *Decision Tree*," *Int. J. Secur.*, no. 11, p. 10, 2020.

[32] A. Bandi and L. Sherpa, *Android Malware Detection Using Machine learning Classifiers*, vol. 141, no. January. Springer Singapore, 2023. doi: 10.1007/978-981-19-3035-5_15.

[33] 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. Informatics J.*, vol. 24, no. 2, pp. 313–325, 2023, doi: 10.1016/j.eij.2023.05.002.

[34] S. R. T. Mat, M. F. A. Razak, M. N. M. Kahar, J. M. Arif, and A. Firdaus, "A Bayesian probability model for Android *malware* detection," *ICT Express*, vol. 8, no. 3, pp. 424–431, 2022, doi: 10.1016/j.icte.2021.09.003.

[35] H. Rathore, A. Samavedhi, S. K. Sahay, and M. Sewak, “Robust *Malware* Detection Models: Learning from Adversarial Attacks and Defenses,” *Forensic Sci. Int. Digit. Investig.*, vol. 37, p. 301183, 2021, doi: 10.1016/j.fsidi.2021.301183.

[36] M. Dener, G. Ok, and A. Orman, “*Malware* Detection Using Memory Analysis Data in Big Data Environment,” *Appl. Sci.*, vol. 12, no. 17, 2022, doi: 10.3390/app12178604.

[37] S. Chormunge and S. Jena, “Correlation based feature selection with clustering for high dimensional data,” *J. Electr. Syst. Inf. Technol.*, vol. 5, no. 3, pp. 542–549, 2018, doi: 10.1016/j.jesit.2017.06.004.