DETEKSI SERANGAN *MALWARE APK REVERSE TCP* MENGGUNAKAN METODE *ANN (ARTIFICIAL NEURAL NETWORK)* PADA *SMALL BOARD COMPUTER*

SKRIPSI

OLEH :

Muhamad Bagas Firmansyah

09011282126035

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

Deteksi Serangan Malware Apk Reverse Tcp Menggunakan Metode ANN (Artificial Neural Network) pada Small Board Computer

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

MUHAMAD BAGAS FIRMANSYAH

09011282126035

Pembimbing 1	**:**	**Prof. Deris Stiawan, S.Kom., M.T., Ph.D.**
		NIP. 197806172006041002
Pembimbing 2	**:**	**Adi Hermansyah, S.Kom., M.T.**
		NIP. 198904302024211001

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T
196612032006041001

AUTHENTICATION PAGE

FINAL TASK

Detection of Reverse TCP APK Malware Attacks Using the ANN (Artificial Neural Network) Method on a Small Board Computer

Submitted in Partial Fulfillment of Requirements for the

Degree of Bachelor of Computer Science

By:

MUHAMAD BAGAS FIRMANSYAH

09011282126035

Supervisor 1	**:**	**Prof. Deris Stiawan, S.Kom., M.T., Ph.D.**
		NIP. 197806172006041002
Co - Supervisor 2	**:**	**Adi Hermansyah, S.Kom., M.T.**
		NIP. 198904302024211001

Acknowledge

Head of Computer System Departement

Dr. Ir. Sukemi, M.T
196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 25 Juli 2025

Tim Penguji :

1. Ketua : Dr. Ir. Ahmad Heryanto, M.T.,
2. Penguji : Kemahyanto Exaudi, M.T.
3. Pembimbing I : Prof. Ir. Deris Stiawan, M.T., Ph.D.
4. Pembimbing II : Adi Hermansyah, S.Kom., M.T.

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Muhamad Bagas Firmansyah

NIM : 09011282126035

Judul : Deteksi Serangan Malware Apk Reverse Tcp Menggunakan Metode ANN (Artificial Neural Network) pada Small Board Computer

Hasil Pengecekan Plagiat/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 laporan tugas akhir ini, maka saya menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.

Palembang, 2025

Yang Menyatakan

Muhamad Bagas Firmansyah

NIM. 09011282126035

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Allah SWT karena atas rahmat dan karunia-Nya, penulisan tugas akhir yang berjudul "Deteksi Serangan Malware APK *Reverse TCP* Menggunakan Metode ANN (Artificial Neural Network) pada Small Board Computer" dapat diselesaikan dengan baik. Penulisan ini disusun sebagai salah satu syarat untuk menyelesaikan program studi dan memperoleh gelar sarjana di Universitas Sriwijaya.

Dalam penulisan tugas akhir ini, penulis berusaha memberikan kontribusi di bidang keamanan siber dengan mengembangkan model deteksi serangan malware berbasis metode *Artificial Neural Network*yang diimplementasikan pada perangkat Small Board Computer. Penelitian ini diharapkan dapat memberikan manfaat dalam meningkatkan kemampuan mitigasi ancaman siber, khususnya serangan malware dengan teknik *Reverse TCP*.

Penulis menyadari bahwa tugas akhir ini tidak akan terselesaikan tanpa bimbingan, dukungan, dan bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT yang telah memberi rahmat, berkah, rejeki, nikmat, dan kesehatan hingga dapat memberi kesempatan bagi penulis untuk menyelesaikan tugas akhir ini.
2. Kedua orang tua, bapak dan ibu yang telah memberikan dukungan dan selalu mendoakan yang terbaik untuk penulis hingga bisa membuat penulis fokus untuk menyelesaikan tugas akhir ini.
3. Kakak dan adik yang selalu membantu penulis waktu ada masalah dan membantu dalam hal-hal kecil di waktu penulis sedang sibuk.
4. Bapak Prof. Dr. Erwin, S.Si., M.Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya, atas dukungan dan fasilitas yang diberikan selama proses studi.

5. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D., dan Adi Hermansyah, S.Kom., M.T., selaku Dosen Pembimbing, yang telah meluangkan waktu untuk memberikan bimbingan terbaik, motivasi, serta saran yang sangat berarti dalam penyelesaian tugas akhir ini.
6. Teman-teman saya Dhani, Arman, Fakhri, Resti, Luluk, Aldi, Dzaky, dan Andrian yang telah memberi penyemangat waktu dalam kegalauan dan bantuan kepada penulis waktu dalam kesusahan.
7. Kak Angga selaku admin Jurusan Sistem Komputer yang telah membantu perihal pemberkasan yang diperlukan penulis.
8. Dan seluruh pihak yang tidak bisa disebutkan satu per satu telah memberikan dukungan, doa, dan saran serta motivasi bagi penulis untuk bisa menyelesaikan proposal tugas akhir ini.

Penulis menyadari bahwa tugas akhir ini masih memiliki kekurangan, baik dari segi isi maupun penulisan. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan untuk perbaikan di masa mendatang.

Akhir kata, semoga tugas akhir ini dapat bermanfaat bagi pembaca dan memberikan kontribusi positif dalam pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber.

Palembang, Juli 2025
Penulis,

Muhamad Bagas Firmansyah
NIM. 09011282126035

DETEKSI SERANGAN *MALWARE APK REVERSE TCP* MENGGUNAKAN METODE *ANN (ARTIFICIAL NEURAL NETWORK)* PADA *SMALL BOARD COMPUTER*

Muhamad Bagas Firmansyah (090112982126035)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: 09011282126035@student.unsri.ac.id

ABSTRAK

Peningkatan penggunaan perangkat Android turut mendorong berkembangnya ancaman keamanan, salah satunya melalui teknik serangan *Reverse TCP* yang memungkinkan akses jarak jauh secara tersembunyi oleh pihak tidak sah. Penelitian ini bertujuan mengembangkan sistem deteksi malware berbasis metode *Artificial Neural Network* (ANN) yang diimplementasikan pada perangkat *Small Board Computer* (SBC) *Banana Pi BPI-R1*. Data diperoleh melalui simulasi serangan *Reverse TCP* menggunakan Metasploit, kemudian dianalisis menggunakan CICFlowMeter dan diproses untuk pelatihan model ANN. Hasil pengujian menunjukkan bahwa model ANN mampu mendeteksi aktivitas serangan dengan akurasi sebesar 98,95%, precision 98,92%, recall 99,33%, dan F1-score 99,12%. Sistem ini juga berhasil membedakan lalu lintas jaringan normal dan berbahaya secara efektif serta menunjukkan performa deteksi yang lebih baik dibandingkan IDS berbasis rule seperti Snort dan Suricata. Implementasi pada perangkat dengan spesifikasi terbatas membuktikan bahwa metode ANN dapat diandalkan sebagai solusi deteksi *malware*.

Kata Kunci: Reverse TCP, Malware Android, *Artificial Neural Network* (ANN), *Small Board Computer*, Deteksi Intrusi.

Detection of Reverse TCP APK Malware Attacks Using the ANN (Artificial Neural Network) Method on a Small Board Computer

Muhamad Bagas Firmansyah (090112982126035)
Department of Computer Systems, Faculty of Computer Science, Sriwijaya University
Email: 09011282126035@student.unsri.ac.id

ABSTRACT

The increasing use of Android devices has also led to the rise of security threats, one of which is the Reverse TCP attack technique that enables unauthorized remote access to victim devices. This study aims to develop a malware detection system using the Artificial Neural Network (ANN) method, implemented on a Small Board Computer (SBC), specifically the Banana Pi BPI-R1. Data was collected through simulated Reverse TCP attacks using Metasploit, analyzed with CICFlowMeter, and processed for ANN model training. The testing results showed that the ANN model successfully detected attack activity with an accuracy of 98.95%, precision of 98.92%, recall of 99.33%, and an F1-score of 99.12%. The system effectively distinguished between normal and malicious network traffic and demonstrated superior detection performance compared to rule-based IDS tools such as Snort and Suricata. Its implementation on a resource-constrained device confirms that the ANN method is a reliable and efficient solution for malware detection.

Keywords: Reverse TCP, Android Malware, Artificial Neural Network (ANN), Small Board Computer, Intrusion Detection System.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di tengah perkembangan teknologi digital yang semakin pesat, ancaman terhadap keamanan informasi juga terus berkembang, salah satunya melalui serangan *malware*. *Malware* mencakup berbagai bentuk perangkat lunak berbahaya seperti virus, *trojan*, *ransomware*, dan *spyware*, yang dapat mengakibatkan kerusakan serius pada data, sistem, dan infrastruktur teknologi informasi. Berdasarkan penelitian Kaspersky Labs [1], jutaan perangkat komputer di seluruh dunia menjadi korban serangan *malware* setiap tahunnya, dan jumlah varian *malware* terus meningkat dari waktu ke waktu. Kompleksitas dan keragaman jenis serangan ini menentang keefektifan metode deteksi tradisional, seperti analisis berbasis tanda tangan (signature-based analysis), yang sering kali tidak mampu mendeteksi ancaman baru. Oleh karena itu, diperlukan solusi deteksi yang lebih canggih, adaptif, dan efektif untuk menghadapi ancaman-ancaman mutakhir, termasuk teknik *Reverse TCP* yang kerap dimanfaatkan penyerang untuk mengakses sistem secara ilegal, khususnya pada platform *android*.

Pada penelitian [2] platform *android* sebagai sistem operasi yang mendominasi lebih dari 70% pangsa pasar perangkat seluler, menjadi target utama serangan siber. Sifatnya yang terbuka dan fleksibel memberikan keuntungan besar bagi pengembang untuk melakukan modifikasi sesuai kebutuhan, namun disisi lain membuka celah keamanan yang signifikan. Serangan berbasis *malware android* tidak hanya berdampak pada pengguna individu, tetapi juga berimplikasi pada organisasi, terutama jika serangan tersebut digunakan untuk mencuri data sensitif atau merusak infrastruktur jaringan. Salah satu teknik serangan yang banyak digunakan adalah payload *Reverse TCP*, yang memungkinkan penyerang mengakses perangkat korban secara jarak jauh tanpa terdeteksi langsung oleh sistem keamanan [3]. Teknik ini membuka peluang bagi pelaku ancaman untuk melakukan pencurian data, pengambilalihan perangkat, atau bahkan penyebaran serangan lanjutan dalam jaringan .

Pada penelitian [4] metode berbasis kecerdasan buatan, seperti *Artificial Neural Network(*ANN*)*, menawarkan potensi besar dalam mendeteksi serangan *malware*. ANN terinspirasi oleh cara kerja otak manusia yang mampu mengenali pola-pola kompleks dan non-linear. Dalam konteks deteksi *malware*, ANN dapat digunakan untuk menganalisis berbagai karakteristik unik dari *malware* dan membedakanya dari aktivitas normal pada jaringan. Penelitian sebelumnya menunjukkan bahwa metode berbasis ANN mampu mencapai akurasi yang sangat tinggi dalam deteksi intrusi dan *malware*. Sebagai contoh, beberapa studi telah melaporkan bahwa ANN dapat mencapai akurasi hingga 99% pada dataset benchmark seperti NSL-KDD dan CICIDS2017.

Pada platform *android*, ANN dapat dimanfaatkan untuk menganalisis fitur-fitur statis dan dinamis dari aplikasi, seperti pola panggilan API, izin aplikasi, hingga perilaku jaringan. Pendekatan seperti *Convolutional Neural Network* (CNN) di penelitian [5] telah digunakan untuk memproses data *malware* menjadi representasi metriks atau gambar, memungkinkan sistem membedakan aplikasi berbahaya dari yang normal dengan tingkat akurasi lebih dari 98%. Selain itu, pendekatan berbasis *Long Short-Term Memory* (*LSTM*) seperti pada penelitian [6] juga telah digunakan secara efektif untuk mendeteksi pola serangan berurutan, seperti *Reverse TCP*, dengan memanfaatkan kemampuannya dalam memproses data yang berurutan.

Penggunaan *Small Board Computer (*SBC*)* sebagai platform untuk menerapkan sistem deteksi berbasis ANN juga memberikan keunggulan tersendiri. SBC, seperti Raspberry Pi dan Jetson Nano, merupakan perangkat komputasi yang ringan, hemat energi, dan berbiaya rendah, menjadikannya ideal untuk implementasi dalam sistem deteksi *malware* di lingkungan nyata. Dengan kemampuan pemrosesan data secara real-time, SBC memungkinkan penerapan sistem deteksi cerdas yang responsif terhadap ancaman, terutama dalam lingkungan rumahan. Penelitian [7] menunjukkan bahwa SBC dapat diintegrasikan dengan perangkat keras lainnya untuk mendeteksi ancaman secara cepat dan efisien.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengembangkan sistem deteksi *malware* berbasis ANN yang diimplementasikan pada perangkat SBC untuk mendeteksi serangan *Reverse TCP*. Pendekatan ini diharapkan tidak hanya meningkatkan keamanan perangkat *Android*, tetapi juga memberikan kontribusi signifikan dalam pengembangan aplikasi kecerdasan buatan pada sistem dengan keterbatasan sumber daya. Sehingga dari latar belakang yang telah dijelaskan, maka penulis ingin mengambil judul "**Deteksi Serangan *Malware* APK *Reverse TCP* Menggunakan Metode ANN (*Artificial Neural Network*) Pada *Small Board Computer***" dengan harapan metode ANN mampu mendeteksi serangan dengan baik pada SBC.

1.2 Rumusan Masalah

Rumusan masalah yang didapatkan dari latar belakang di atas sebagai berikut:

1. Bagaimana mendeteksi serangan malware Reverse TCP pada perangkat Android secara efektif?
2. Bagaimana penerapan metode Artificial Neural Network (ANN) dalam sistem deteksi serangan malware Reverse TCP?
3. Bagaimana mengevaluasi kinerja sistem deteksi ANN dalam membedakan lalu lintas jaringan normal dan berbahaya?

1.3 Batasan Masalah

Batasan masalah untuk penelitian ini sebagai berikut:

1. Penelitian difokuskan pada serangan malware berbasis APK dengan teknik *Reverse TCP*.
2. Deteksi dilakukan menggunakan metode *Artificial Neural Network* (ANN) saja.
3. Sistem diimplementasikan dan diuji hanya pada perangkat Small Board Computer (SBC).

1.4 Tujuan

Tujuan dari penelitian ini berdasarkan rumusan masalah di atas sebagai berikut:

1. Mengembangkan model *Artificial Neural Network* (ANN) untuk mendeteksi serangan malware *Reverse TCP* pada perangkat Android.
2. Mengimplementasikan sistem deteksi berbasis ANN ke dalam Small Board Computer (SBC).
3. Mengevaluasi kinerja sistem menggunakan metrik akurasi, presisi, recall, dan F1-score berdasarkan data serangan nyata.

1.5 Manfaat

Manfaat penelitian ini adalah sebagai berikut:

1. Memberikan solusi deteksi malware *Reverse TCP* menggunakan metode ANN.
2. Menunjukkan efektivitas ANN pada perangkat dengan sumber daya terbatas seperti SBC.
3. Menjadi referensi dalam pengembangan sistem keamanan jaringan berbasis AI.

1.6 Metodologi Penelitian

Pada penelitian ini memiliki berapa tahapan:

1. Studi Pustaka / Literatur

   Merupakan proses pencarian referensi dari berbagai sumber kajian ilmiah, seperti artikel, jurnal, dan buku yang relevan dengan penelitian yang akan dilaksanakan.

2. Pengumpulan Data

   Data yang digunakan dalam penelitian ini meliputi data fitur statis dan dinamis dari aplikasi *android*. Data fitur statis mencakup informasi seperti izin aplikasi dan struktur APK, sementara data fitur dinamis mencakup pola perilaku aplikasi dalam jaringan, termasuk penggunaan *Reverse TCP*. Sumber data dapat berasal dari dataset publik, hasil simulasi, atau pengujian langsung.

3. Pra-pemrosesan Data

   Tahap ini mencakup proses pembersihan dan normalisasi data agar

sesuai dengan format yang diperlukan untuk pelatihan model ANN. Data mentah yang diperoleh dari fitur statis dan dinamis akan diekstraksi, diolah, dan dikategorikan menjadi aktivitas normal dan aktivitas berbahaya.

4. Perancangan Model ANN

   Pada tahap ini, model *Artificial Neural Network*(ANN) dirancang untuk mendeteksi *malware* berbasis *Reverse TCP*. Desain model mencakup pemilihan arsitektur jaringan, seperti jumlah lapisan tersembunyi, fungsi aktivasi, serta parameter pelatihan seperti learning rate dan jumlah epoch.

5. Pelatihan dan Pengujian Model

   Model ANN dilatih menggunakan dataset yang telah diproses. Dataset akan dibagi menjadi data pelatihan dan data pengujian untuk mengevaluasi kinerja model. Metode validasi, seperti k-fold cross-validation, digunakan untuk memastikan hasil pelatihan yang andal.

6. Implementasi pada *Small Board Computer* (SBC)

   Model ANN yang telah dilatih diimplementasikan pada perangkat *Small Board Computer* (SBC). Proses ini melibatkan pengoptimalan agar sistem dapat berjalan dengan baik di perangkat dengan keterbatasan sumber daya komputasi.

7. Pengujian Sistem

   Sistem deteksi *Malware* yang telah diimplementasikan akan diuji dalam kondisi nyata untuk mengukur akurasi, efisiensi, dan kemampuan real-time dalam mendeteksi serangan *Reverse TCP*.

8. Analisis dan Evaluasi

   Hasil pengujian dianalisis untuk mengevaluasi kinerja sistem berdasarkan metrik seperti akurasi, precision, recall, dan F1-score. Jika diperlukan, model akan dioptimalkan lebih lanjut untuk meningkatkan performanya.

9. Kesimpulan

   Hasil akhir penelitian disimpulkan, termasuk temuan-temuan utama dan implikasi praktisnya. Seluruh proses dan hasil penelitian didokumentasikan secara rinci untuk keperluan publikasi atau pengembangan lanjutan.

1.7 Sistematika Penulisan

Sistematika penulisan disusun untuk memperjelas dan menegaskan setiap bab yang akan dibahas dalam penelitian ini. Berikut adalah sistematika penulisan yang akan digunakan:

Bab I: Pendahuluan

Bab ini berisi latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, serta sistematika penulisan. Bab ini memberikan gambaran umum mengenai topik yang akan dibahas dalam penelitian ini.

Bab II: Tinjauan Pustaka

Bab ini menyajikan kajian teori terkait dengan topik penelitian, termasuk konsep dasar mengenai *malware*, jenis-jenis *malware* APK, teknik *Reverse TCP*, serta metode deteksi *malware* menggunakan *Artificial Neural Network*(ANN). Selain itu, bab ini juga membahas penelitian terdahulu yang relevan dengan topik ini.

Bab III: Metodologi Penelitian

Bab ini menjelaskan secara rinci tentang pendekatan dan metode yang digunakan dalam penelitian, mulai dari pengumpulan data, pra-pemrosesan data, perancangan model ANN, pelatihan dan pengujian model, implementasi pada *Small Board Computer* (SBC), hingga pengujian dan evaluasi sistem yang dikembangkan.

Bab IV: Hasil dan Pembahasan

Bab ini menyajikan hasil eksperimen dan pengujian yang telah dilakukan, termasuk analisis terhadap kinerja model ANN dalam mendeteksi *malware Reverse TCP*. Hasil evaluasi sistem yang diterapkan pada perangkat SBC juga dibahas di sini.

Bab V: Kesimpulan dan Saran

Bab ini memberikan kesimpulan dari hasil penelitian yang telah dilakukan dan menyarankan langkah-langkah pengembangan lebih lanjut terkait dengan deteksi *malware* pada perangkat *android* menggunakan metode ANN.

DAFTAR PUSTAKA

[1] A. H. Thiziers, K. Tiémoman, N. B. Gérard, and T. T. Q. Kabir, "Malware Detection Using Deep Learning," *Open J. Appl. Sci.*, vol. 13, no. 12, pp. 2480–2491, 2023, doi: 10.4236/ojapps.2023.1312193.

[2] 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.

[3] Y. Kolli, T. K. Mohd, and A. Y. Javaid, "Remote Desktop Backdoor Implementation with *Reverse TCP* Payload using Open Source Tools for Instructional Use".

[4] M. Choraś and M. Pawlicki, "Intrusion detection approach based on optimised artificial neural network," *Neurocomputing*, vol. 452, pp. 705–715, 2021, doi: 10.1016/j.neucom.2020.07.138.

[5] L. N. Vu and S. Jung, "AdMat: A CNN-on-Matrix Approach to Android Malware Detection and Classification," *IEEE Access*, vol. 9, pp. 39680–39694, 2021, doi: 10.1109/ACCESS.2021.3063748.

[6] M. Kumar, S. Singh, U. Pilania, G. Arora, and M. Jain, "LSTM-based Approach for Android Malware Detection," *Procedia Comput. Sci.*, vol. 230, no. 2023, pp. 679–687, 2023, doi: 10.1016/j.procs.2023.12.123.

[7] S. J. Matthews, R. W. Blaine, and A. F. Brantly, "Evaluating single board computer clusters for cyber operations," *2016 IEEE Int. Conf. Cyber Conflict, CyCon U.S. 2016*, no. February 2018, 2017, doi: 10.1109/CYCONUS.2016.7836622.

[8] N. Tarar, S. Sharma, and C. R. Krishna, "Analysis and Classification of Android Malware using Machine Learning Algorithms," in *2018 3rd International Conference on Inventive Computation Technologies (ICICT)*, 2018, pp. 738–743. doi: 10.1109/ICICT43934.2018.9034337.

[9] B. Ramadhan, Y. Purwanto, and M. F. Ruriawan, "Forensic malware identification using naive bayes method," *2020 Int. Conf. Inf. Technol. Syst. Innov. ICITSI 2020 - Proc.*, pp. 1–7, 2020, doi:

10.1109/ICITSI50517.2020.9264959.

[10] H. R. Sandeep, “Static analysis of android malware detection using deep learning,” *2019 Int. Conf. Intell. Comput. Control Syst. ICCS 2019*, no. Iciccs, pp. 841–845, 2019, doi: 10.1109/ICCS45141.2019.9065765.

[11] 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*, pp. 8–12, 2020, doi: 10.1109/ICIMCIS51567.2020.9354315.

[12] F. Shang, Y. Li, X. Deng, and D. He, “Android malware detection method based on naive bayes and permission correlation algorithm,” *Cluster Comput.*, vol. 21, no. 1, pp. 955–966, 2017, doi: 10.1007/s10586-017-0981-6.

[13] M. A. Khalifa, A. Elsayed, A. Hussien, and A. S. Hussainy, “Android Malware Detection and Prevention Based on Deep Learning and Tweets Analysis,” in *2024 6th International Conference on Computing and Informatics (ICCI)*, IEEE, Mar. 2024, pp. 153–157. doi: 10.1109/ICCI61671.2024.10485022.

[14] P. Toupas, D. Chamou, K. M. Giannoutakis, A. Drosou, and D. Tzovaras, “An intrusion detection system for multi-class classification based on deep neural networks,” *Proc. - 18th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2019*, pp. 1253–1258, 2019, doi: 10.1109/ICMLA.2019.00206.

[15] Z. Fang, J. Liu, R. Huang, P. Chen, X. Li, and X. Chen, “Research on Multi-model Android Malicious Application Detection Based on Feature Fusion,” in *2021 4th International Conference on Robotics, Control and Automation Engineering (RCAE)*, IEEE, Nov. 2021, pp. 147–151. doi: 10.1109/RCAE53607.2021.9638928.

[16] P. Singh, T. Hasija, and K. Ramkumar, “Malware Classification for Enhanced Android Permissions: A Comparative Study of SVM Kernel and Voting Classifier,” in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, IEEE, Jun. 2024, pp. 1–6. doi: 10.1109/ICCCNT61001.2024.10724764.

[17] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, and K. M. Koumadi, “Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN),” *J. Comput. Networks Commun.*, vol. 2019, 2019, doi: 10.1155/2019/4683982.

[18] P. Freitas De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo, and F. L. Soares, “An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks with a Low-Cost Platform,” *IEEE Access*, vol. 9, pp. 166855–166869, 2021, doi: 10.1109/ACCESS.2021.3136147.

[19] T. Saba, T. Sadad, A. Rehman, Z. Mehmood, Q. Javaid, and F. Works, “Intrusion Detection System Through Advance Machine Learning for the Internet of Things Networks,” no. April, 2021.

[20] G. Karat, J. M. Kannimoola, N. Nair, A. Vazhayil, V. G. Sujadevi, and P. Poornachandran, “CNN-LSTM Hybrid Model for Enhanced Malware Analysis and Detection,” *Procedia Comput. Sci.*, vol. 233, pp. 492–503, 2024, doi: 10.1016/j.procs.2024.03.239.

[21] 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.

[22] R. A. Abed, E. K. Hamza, and A. J. Humaidi, “A modified CNN-IDS model for enhancing the efficacy of intrusion detection system,” *Meas. Sensors*, vol. 35, no. October 2023, p. 101299, 2024, doi: 10.1016/j.measen.2024.101299.

[23] H. Q. Gheni and W. L. Al-Yaseen, “Two-step data clustering for improved intrusion detection system using CICIoT2023 dataset,” *e-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 9, no. March, p. 100673, 2024, doi: 10.1016/j.prime.2024.100673.

[24] C. Rajathi and P. Rukmani, “Hybrid Learning Model for intrusion detection system: A combination of parametric and non-parametric classifiers,” *Alexandria Eng. J.*, vol. 112, no. November 2024, pp. 384–396, 2025, doi:

10.1016/j.aej.2024.10.101.

[25] N. Borgioli, F. Aromolo, L. Thi Xuan Phan, and G. Buttazzo, “A convolutional autoencoder architecture for robust network intrusion detection in embedded systems,” *J. Syst. Archit.*, vol. 156, no. February, p. 103283, 2024, doi: 10.1016/j.sysarc.2024.103283.

[26] D. Arivudainambi, V. K. Varun, S. C. S., and P. Visu, “Malware traffic classification using principal component analysis and *Artificial Neural Network*for extreme surveillance,” *Comput. Commun.*, vol. 147, no. August, pp. 50–57, 2019, doi: 10.1016/j.comcom.2019.08.003.

[27] P. Moll, S. Theuermann, and H. Hellwagner, “Persistent interests in named data networking,” *IEEE Veh. Technol. Conf.*, vol. 2018-June, pp. 1–5, 2018, doi: 10.1109/VTCSpring.2018.8417861.

[28] P. D. Meshram and R. C. Thool, “A survey paper on vulnerabilities in android OS and security of android devices,” *Proc. - 2014 IEEE Glob. Conf. Wirel. Comput. Networking, GCWCN 2014*, vol. 03, no. 004, pp. 174–178, 2015, doi: 10.1109/GCWCN.2014.7030873.

[29] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, and S. Dolev, “Google Android: A State-of-the-Art Review of Security Mechanisms,” 2009, [Online]. Available: http://arxiv.org/abs/0912.5101

[30] M. S. Haq, M. Samani, Karwanto, and N. Hariyati, “Android-Based Digital Library Application Development,” *Int. J. Interact. Mob. Technol.*, vol. 16, no. 11, pp. 224–237, 2022, doi: 10.3991/ijim.v16i11.32055.

[31] A. P. Namanya, A. Cullen, I. U. Awan, and J. P. Disso, “The World of Malware: An Overview,” *Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud, FiCloud 2018*, pp. 420–427, 2018, doi: 10.1109/FiCloud.2018.00067.

[32] 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*, pp. 444–450, 2018, doi: 10.1109/IEMCON.2018.8614801.

[33] C. Atwell, T. Blasi, and T. Hayajneh, "*Reverse TCP* and Social Engineering Attacks in the Era of Big Data," *Proc. - 2nd IEEE Int. Conf. Big Data Secur. Cloud, IEEE BigDataSecurity 2016, 2nd IEEE Int. Conf. High Perform. Smart Comput. IEEE HPSC 2016 IEEE Int. Conf. Intell. Data S*, pp. 90–95, 2016, doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.60.

[34] O. Valea and C. Oprisa, "Towards Pentesting Automation Using the Metasploit Framework," *Proc. - 2020 IEEE 16th Int. Conf. Intell. Comput. Commun. Process. ICCP 2020*, pp. 171–178, 2020, doi: 10.1109/ICCP51029.2020.9266234.

[35] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," *CINTI 2014 - 15th IEEE Int. Symp. Comput. Intell. Informatics, Proc.*, pp. 237–242, 2014, doi: 10.1109/CINTI.2014.7028682.

[36] P. Mestry and A. Rathi, "Deep learning-Based Real-time malicious network traffic detection system for Cyber-Physical Systems," in *2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, 2022, pp. 1–9. doi: 10.1109/ICBDS53701.2022.9935854.

[37] B. H. Ali, N. Sulaiman, S. A. R. Al-Haddad, R. Atan, and S. L. M. Hassan, "DDoS Detection Using Active and Idle Features of Revised CICFlowMeter and Statistical Approaches," in *2022 4th International Conference on Advanced Science and Engineering (ICOASE)*, 2022, pp. 148–153. doi: 10.1109/ICOASE56293.2022.10075591.

[38] B. Hsupeng, K.-W. Lee, T.-E. Wei, and S.-H. Wang, "Explainable Malware Detection Using Predefined Network Flow," in *2022 24th International Conference on Advanced Communication Technology (ICACT)*, 2022, pp. 27–33. doi: 10.23919/ICACT53585.2022.9728897.

[39] W. J. Tay, S. L. Lew, and S. Y. Ooi, "Remote Access VPN using Mikrotik Router," in *2022 International Conference on Computer and Drone Applications (IConDA)*, 2022, pp. 119–124. doi: 10.1109/ICONDA56696.2022.10000334.

[40] Susanto, A. F. Daru, and F. W. Christanto, "Packet Filtering Gateway and

Application Layer Gateway on Mikrotik Router Based Firewalls for Server and Internet Access Restrictions," in *2023 International Conference on Technology, Engineering, and Computing Applications (ICTECA)*, 2023, pp. 1–6. doi: 10.1109/ICTECA60133.2023.10490754.

[41] Y. Gao, S. Liu, and L. Yang, "Artificial intelligence and innovation capability: A dynamic capabilities perspective," *Int. Rev. Econ. Financ.*, vol. 98, no. August 2024, p. 103923, 2025, doi: 10.1016/j.iref.2025.103923.

[42] G. Qu and H. Jing, "Is new technology always good ? Artificial intelligence and corporate tax avoidance : Evidence from China," *Int. Rev. Econ. Financ.*, vol. 98, no. November 2024, p. 103949, 2025, doi: 10.1016/j.iref.2025.103949.

[43] A. Baliyan, K. S. Kaswan, and J. S. Dhatterwal, "An Empirical Analysis of Python Programming for Advance Computing," in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2022, pp. 1482–1486. doi: 10.1109/ICACITE53722.2022.9823643.

[44] S. Kumar, S. Gupta, and S. Arora, "Research Trends in Network-Based Intrusion Detection Systems: A Review," *IEEE Access*, vol. 9, pp. 157761–157779, 2021, doi: 10.1109/ACCESS.2021.3129775.