DETEKSI POLA SERANGAN ANDROID MALWARE MENGGUNAKAN METODE *CONVOLUTIONAL NEURAL NETWORK (CNN)*

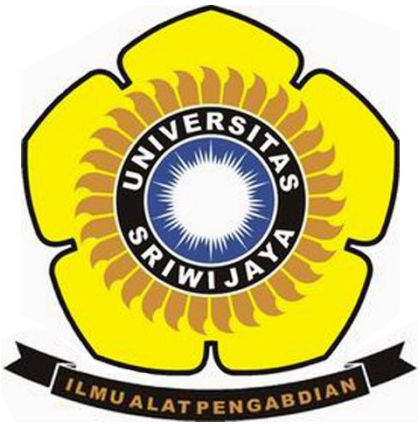
OLEH :
REZA MAULANA
NIM. 09012682125017

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2025

DETEKSI POLA SERANGAN ANDROID MALWARE MENGGUNAKAN METODE *CONVOLUTIONAL NEURAL NETWORK (CNN)*

TESIS

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister



OLEH :
REZA MAULANA
NIM. 09012682125017

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2025

LEMBAR PENGESAHAN

DETEKSI POLA SERANGAN ANDROID MALWARE MENGGUNAKAN METODE *CONVOLUTIONAL NEURAL NETWORK (CNN)*

TESIS

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister

OLEH :
REZA MAULANA
NIM. 09012682125017

Palembang, 2 Juni 2025

Pembimbing

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Mengetahui,
Ketua Program Studi Magister Ilmu Komputer

Dr. Firdaus, M.Kom
NIP. 197801212008121003

HALAMAN PERSETUJUAN

Pada hari Jumat, 23 Mei 2025 telah dilaksanakan ujian sidang tesis di depan dewan penguji pada program studi Magister Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya, atas nama :

N a m a : Reza Maulana

N I M : 09012682125017

Judul : Deteksi Pola Serangan Android Malware Menggunakan Metode *Convolutional Neural Network* (CNN)

1. Ketua Penguji

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

2. Penguji I

   Dr. Ahmad Zarkasi, M.T. :.....
   NIP. 197908252023211007

3. Penguji II

   Dr. Ahmad Heryanto, M.T. :.....
   NIP. 198701222015041002

4. Pembimbing

   Prof. Deris Stiawan, M.T., Ph.D. :.....
   NIP. 197806172006041002

Mengetahui,

Ketua Program Studi Magister Ilmu Komputer

Dr. Eirdaus, M.Kom

NIP. 197801212008121003

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Reza Maulana
NIM	: 09012682125017
Program Studi	: S2 Magister Ilmu Komputer
Judul Tesis	: Deteksi Pola Serangan Android Malware Menggunakan Metode *Convolutional Neural Network* (CNN)

Hasil Pengecekan Software iThenticate/Turnitin : **19%**

Menyatakan bahwa laporan tesis saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tesis ini, maka saya bersedia menerima sanksi akademik dari universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 14 Mei 2025

Reza Maulana

NIM. 09012682125017

Detection of Android Malware with Deep Learning Method using Convolutional Neural Network Model

Reza Maulana

ABSTRACT

Android malware is an application that targets Android devices to steal crucial data, including money or confidential information from Android users. Recent years have seen a surge in research on Android malware, as its types continue to evolve, and cybersecurity requires periodic improvements. This research focuses on detecting Android malware attack patterns using deep learning and convolutional neural network (CNN) models, which classify and detect malware attack patterns on Android devices into two categories: malware and non-malware. This research contributes to understanding how effective the CNN models are by comparing the ratio of data used with several epochs. We effectively use CNN models to detect malware attack patterns. The results show that the deep learning method with the CNN model can manage unstructured data. The research results indicate that the CNN model demonstrates a minimal error rate during evaluation. The comparison of accuracy, precision, recall, F1 Score, and area under the curve (AUC) values demonstrates the recognition of malware attack patterns, reaching an average of 92% accuracy in data testing. This provides a holistic understanding of the model's performance and its practical utility in detecting Android malware, for future building of cyber applications.

Keywords: Android Malware; Classification; CNN; Deep Learning; Pattern Recognition.

Palembang, June 2025

Acknowledged by,
Head of
Master of Computer Science Program

Dr. Firdaus, M.Kom
NIP. 197801212008121003

Supervisor

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Deteksi Pola Serangan Android Malware Menggunakan Metode *Convolutional Neural Network* (CNN)

Reza Maulana

ABSTRAK

Malware Android adalah aplikasi yang menargetkan perangkat Android untuk mengambil data penting, termasuk keuangan atau informasi rahasia dari pengguna Android. Beberapa tahun terakhir telah banyak penelitian yang membahas tentang malware Android, karena jenisnya terus berkembang, dan keamanan siber memerlukan peningkatan secara berkala. Penelitian ini berfokus pada pendeteksian pola serangan malware Android menggunakan *deep learning* dan model *Convolutional Neural Network* (CNN), yang mengklasifikasikan dan mendeteksi pola serangan malware pada perangkat Android menjadi dua kategori: malware dan non-malware (*benign*). Penelitian ini berkontribusi untuk memahami seberapa efektif model CNN dengan membandingkan rasio data yang digunakan dengan beberapa *epoch*. Model CNN yang digunakan efektif untuk mendeteksi pola serangan malware. Hasilnya menunjukkan bahwa metode *deep learning* dengan model CNN dapat mengelola data yang tidak terstruktur. Hasil penelitian ini menunjukkan bahwa model CNN menghasilkan tingkat kesalahan minimal selama evaluasi. Perbandingan nilai akurasi, presisi, *recall*, *F1-Score*, dan nilai *Area Under the Curve* (AUC) menunjukkan pengenalan pola serangan malware, mencapai rata-rata akurasi diatas 92% dalam pengujian data. Ini memberikan pemahaman holistik tentang kinerja model dan utilitas praktisnya dalam mendeteksi Malware Android yang selanjutnya dapat digunakan untuk membangun aplikasi keamanan siber.

Kata Kunci: Android Malware; Klasifikasi; CNN; Deep Learning; Pengenalan Pola.

Palembang, Juni 2025

Mengetahui,
Ketua Program Studi
Magister Ilmu Komputer

Dr. Firdaus, M.Kom
NIP. 197801212008121003

Pembimbing,

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

KATA PENGANTAR

Puji syukur Penulis panjatkan kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya sehingga Penulis dapat menyelesaikan tesis dan menyusun laporan tesis yang berjudul "Deteksi Pola Serangan Android Malware Menggunakan Metode *Convolutional Neural Network* (CNN)". Laporan tesis ini disusun untuk memenuhi salah satu persyaratan kelulusan tingkat S2 pada Jurusan Magister Ilmu Komputer Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih yang tak terhingga kepada pihak-pihak telah memberikan dukungan, bimbingan, motivasi dan kemauan kepada penulis untuk menyelesaikan tesis ini, yaitu kepada:

1. Dekan Fakultas Ilmu Komputer Universitas Sriwijaya, Bapak Prof. Dr. Erwin, M.Si.
2. Ketua Program Studi Magister Ilmu Komputer, Bapak Dr. Firdaus, M.Kom
3. Pembimbing Tesis yang sangat saya banggakan, yaitu Prof. Deris Stiawan, M.T., Ph.D.
4. Kedua Orang Tua saya dan motivator pribadi saya dalam penulisan laporan tesis, Ibu Husnawati, M.Kom
5. Teman – teman MIK khususnya angkatan 2021, dan pihak – pihak lain yang membantu dalam penyusunan laporan ini.

Akhir kata Penulis mengucapkan permohonan maaf yang sebesar – besarnya apabila terdapat kesalahan kata maupun kekurangan – kekurangan di dalam penulisan tesis ini. Semoga laporan tesis ini dapat bermanfaat bagi semua pihak yang membutuhkan, serta dapat menambah wawasan dan menunjang perkembangan ilmu pengetahuan khususnya bagi Penulis maupun para Akademisi pada umumnya.

Palembang, April 2025

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB 1 PENDAHULUAN

Pada bab ini berisi latar belakang dilakukannya penelitian yang berjudul: "Deteksi Pola Serangan Android Malware Menggunakan Metode *Convolutional Neural Network* (CNN)". Kemudian dari latar belakang tersebut dapat dirumuskan permasalahan yang akan diangkat, agar permasalahan tidak meluas maka diberikan batasan masalah. Kemudian diberikan tujuan dan manfaat dari penelitian yang dibuat, dan metodologi yang digunakan dalam penelitian tersebut.

1.1 Latar Belakang

Malware Android adalah perangkat lunak berbahaya yang dirancang khusus untuk menargetkan perangkat yang menjalankan sistem operasi Android. (Sharma and Rattan, 2021) Bentuknya bisa bermacam-macam, termasuk virus, trojan, adware, dan spyware (Yadav *et al.*, 2022). Malware Android dapat menginfeksi perangkat melalui berbagai cara, seperti dengan mengunduh aplikasi jahat dari aplikasi pihak ketiga, mengunjungi situs web yang disusupi, atau dengan mengeksploitasi kerentanan di sistem operasi perangkat. Setelah terinstal, malware dapat mencuri informasi pribadi, mengirim pesan SMS yang tidak diinginkan (Yadav *et al.*, 2022), melakukan panggilan telepon tanpa izin, atau melakukan tindakan berbahaya lainnya (Talal *et al.*, 2019).

Pada tahun 2018, ada beberapa malware Android yang terkenal. Salah satu yang paling tersebar luas adalah malware "Joker" (Mercaldo *et al.*, 2022), yang menginfeksi lebih dari 24.000 perangkat Android hanya dalam beberapa bulan. Malware didistribusikan melalui aplikasi pihak ketiga dan disamarkan sebagai aplikasi yang sah (He, Chan and Guizani, 2021), seperti penghemat baterai dan pembaca kode QR. Setelah terinstal, malware akan berlangganan perangkat yang terinfeksi ke layanan premium tanpa sepengetahuan pengguna, mengakibatkan kerugian finansial yang signifikan bagi para korban.

Lainnya adalah malware "Agen Smith", yang ditemukan pada Februari 2018 dan menginfeksi lebih dari 25 juta perangkat Android. Malware didistribusikan melalui iklan pada aplikasi android (He, Chan and Guizani, 2021). Setelah terinstal, malware akan menggantikan aplikasi yang sah pada perangkat dengan versi jahat yang akan menampilkan iklan yang tidak diinginkan dan mengumpulkan informasi pribadi.

Malware lain adalah malware "BlackRock", yang ditemukan pada tahun 2020 (Ning, 2021). Malware tersebut didistribusikan melalui aplikasi pihak ketiga dan disamarkan sebagai aplikasi yang sah, seperti aplikasi keuangan. Setelah terinstal, malware akan mencuri informasi pribadi, termasuk data keuangan dan kredensial login, dan melakukan tindakan berbahaya lainnya.

Secara umum, android malware terus tumbuh dan berkembang, dengan banyak keluarga dan varian baru bermunculan. Penjahat dunia maya semakin fokus pada malware seluler, dengan banyak keluarga dan varian baru bermunculan. Tren ini diperkirakan akan terus berlanjut di masa mendatang karena perangkat seluler menjadi target yang semakin penting bagi penjahat dunia maya.

Salah satu metode yang dapat digunakan malware android adalah keylogging (Waterson, 2020; Hubbard, Bendiab and Shiaeles, 2022), di mana ia mencatat setiap penekanan tombol yang dilakukan pada perangkat, termasuk kata sandi, nomor kartu kredit, dan informasi sensitif lainnya. Metode lainnya adalah scraping (Waterson, 2020), di mana malware mengumpulkan informasi dari berbagai sumber seperti kontak perangkat, kalender, dan log panggilan, serta dari aplikasi yang terpasang di perangkat. Metode lain adalah eksfiltrasi data, di mana malware mengirimkan informasi yang dikumpulkan ke server jarak jauh, di mana informasi tersebut dapat dianalisis dan digunakan untuk tujuan jahat (Hubbard, Bendiab and Shiaeles, 2022).

Dalam beberapa tahun terakhir penerapan metode deep learning dalam mengklasifikasikan pola serangan pada malware telah dilakukan (Wang, 2020) salah satunya adalah penelitian (Ren *et al.*, 2020) pada tahun 2020 yang mendeteksi pola serangan end-to-end malware dengan penerapan metode

DexCNN dan TexCNN, kemudian penelitian yang dilakukan oleh (Pektaş and Acarman, 2020) yang menggunakan metode API Call Graph untuk mendeteksi pola serangan malware.

Dalam beberapa penelitian tersebut deteksi malware pada android menggunakan metode *deep learning* telah menjadi hotspot penelitian di beberapa tahun terakhir, namun kurang detail dan komprehensif sehingga penelitian tersebut terus dikembangkan hingga saat ini (Wang, 2020), Deteksi malware menggunakan metode *deep learning* telah menjadi bidang penelitian yang signifikan dalam beberapa tahun terakhir karena meningkatnya ancaman malware di dunia maya. Tantangan utama dalam pendeteksian malware adalah kemampuan malware untuk berevolusi dengan cepat, sehingga menyulitkan metode pendeteksian tradisional untuk mengimbanginya. metode *deep learning* terbukti sangat efektif dalam mendeteksi malware karena kemampuannya mempelajari fitur dari kumpulan data besar secara otomatis dan beradaptasi dengan ancaman yang muncul.

Salah satu masalah utama dalam deteksi malware berbasis *deep learning* adalah kebutuhan akan kumpulan data yang besar dan beragam untuk melatih model secara efektif. Hal ini dapat menjadi sebuah tantangan, terutama ketika berhadapan dengan sifat malware yang terus berkembang, yang dapat menyebabkan kurangnya data yang relevan untuk pelatihan. Selain itu, kompleksitas malware dapat mempersulit identifikasi fitur paling efektif untuk diekstraksi dari data, sehingga dapat memengaruhi performa model. sehingga pada penelitian ini akan dilakukan "Deteksi Pola Serangan Android Malware Menggunakan Metode *Convolutional Neural Network* (CNN)" untuk menganalisis pola serangan malware yang terdapat pada perangkat android dan mengklasifikasikan serangan malware.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka perumusan masalah pada penelitian ini yaitu;

1. Bagaimana menerapkan metode *Deep Learning Convolutional Neural Network* dalam mengklasifikasikan serangan malware pada perangkat android.
2. Bagaimana menganalisis penerapan metode *Convolutional Neural Network* dalam mengklasifikasi serangan malware android.
3. Bagaimana mengukur efektivitas penerapan metode *Convolutional Neural Network* dalam mengklasifikasi serangan malware android.

1.3 Tujuan Dan Manfaat

Secara umum tujuan dari penelitian ini adalah :

1. Dapat menerapkan metode *deep learning* menggunakan *Convolutional Neural Network* dalam mengklasifikasikan malware android.
2. Dapat menganalisis penerapan metode *deep learning* menggunakan *Convolutional Neural Network* untuk mendeteksi pola serangan malware pada perangkat android.
3. Dapat mengukur efektivitas penerapan metode *Convolutional Neural Network* pada serangan malware yang terdapat pada perangkat android untuk membangun pertahanan sistem.

Manfaat yang dapat diperoleh dari penelitian ini adalah :

1. Hasil analisis dari penerapan metode *deep learning* dalam mengklasifikasikan malware android dapat digunakan sebagai tolak ukur data dalam keamanan siber.
2. Hasil akurasi yang diperoleh dalam penerapan metode *deep learning* pada malware android dapat digunakan untuk mempertimbangkan metode yang tepat dalam pengklasifikasian malware android.
3. Pendeteksian pola serangan dari malware pada android dapat digunakan untuk membentuk pertahanan sistem dalam keamanan siber

1.4 Sistematika Penulisan

Untuk lebih memudahkan dalam menyusun tesis ini dan memperjelas isi dari setiap bab yang ada pada laporan ini, maka dibuatlah sistematika penulisan sebagai berikut:

1. **BAB I Pendahuluan**

   Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi penelitian, dan sistematika penulisan.

2. **BAB II Tinjauan Pustaka**

   Bab ini berisi tentang seluruh penjelasan mengenai landasan teori yang berhubungan dengan permasalahan yang dibahas pada penulisan tesis ini.

3. **BAB III Metodologi Penelitian**

   Bab ini berisi penjelasan secara bertahap dan teperinci tentang langkah-langkah (metodologi) yang digunakan untuk membuat kerangka berfikir dan kerangka kerja dalam menyelesaikan tesis.

4. **BAB IV Analisa dan Pembahasan**

   Bab ini berisi tentang analisa dan pembahasan dari tiap – tiap blok diagram perencanaan rangkaian dan data – data hasil pengukuran.

5. **BAB V Kesimpulan**

   Bab ini berisi kesimpulan tentang hasil yang telah diperoleh serta merupakan jawaban dari tujuan yang ingin dicapai pada bab 1 (pendahuluan).

DAFTAR PUSTAKA

Afifah, N. and Stiawan, D. (2019) 'The Implementation of Deep Neural Networks Algorithm for Malware Classification', *Computer Engineering and Applications Journal*, 8(3), pp. 189–202. doi: 10.18495/comengapp.v8i3.294.

Akhtar, M. S. and Feng, T. (2022) 'Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time', *Symmetry*, 14(11). doi: 10.3390/sym14112308.

Almomani, I., Alkhayer, A. and El-Shafai, W. (2022) 'An Automated Vision-Based Deep Learning Model for Efficient Detection of Android Malware Attacks', *IEEE Access*. ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/abstract/document/9668849/.

Alzubaidi, A. (2021) 'Sustainable Android Malware Detection Scheme using Deep Learning Algorithm', *... Journal of Advanced Computer Science and ...*. search.proquest.com. Available at: https://search.proquest.com/openview/a0ba078716308553aaa68cadeaadc813/1?pq-origsite=gscholar&cbl=5444811.

Bala, Z. (2022) 'Transfer Learning Approach for Malware Images Classification on Android Devices Using Deep Convolutional Neural Network', *Procedia Computer Science*, pp. 429–440. doi: 10.1016/j.procs.2022.11.027.

Bayazit, E. C. and Sahingoz, O. K. (2022) 'A Deep Learning Based Android Malware Detection System with Static Analysis', *... International Congress on ...*. ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/abstract/document/9800057/.

Chen, M. *et al.* (2022) 'An Android Malware Detection Method Using Deep Learning based on Multi-features', *2022 IEEE International ...*. ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/abstract/document/9844642/.

Feng, P. (2018) 'A novel dynamic android malware detection system with ensemble learning', *IEEE Access*, 6, pp. 30996–31011. doi: 10.1109/ACCESS.2018.2844349.

Feng, R. *et al.* (2020) 'A Performance-Sensitive Malware Detection System Using Deep Learning on Mobile Devices', XX(Xx), pp. 1–16.

Gupta, C. *et al.* (2022) 'A Systematic Review on Machine Learning and Deep Learning', *Progress in Biophysics and Molecular Biology*, (June). Available at: https://doi.org/10.1016/j.pbiomolbio.2022.07.004.

Hadiprakoso, R. B., Qomariasih, N. and Yasa, R. N. (2021) 'Identifikasi Malware Android Menggunakan Pendekatan Analisis Hibrid Dengan Deep Learning', *Jurnal Teknologi Informasi Universitas Lambung Mangkurat (JTIULM)*, 6(2), pp. 77–84. doi: 10.20527/jtiulm.v6i2.82.

He, D., Chan, S. and Guizani, M. (2021) 'Mobile application security: Malware threats and defenses', *IEEE Wireless Communications*, 22(1), pp. 138–144. doi: 10.1109/MWC.2015.7054729.

Hubbard, J., Bendiab, G. and Shiaeles, S. (2022) 'IPASS: A Novel Open-Source Intelligence Password Scoring System', *Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience, CSR 2022*. IEEE, pp. 90–95. doi: 10.1109/CSR54599.2022.9850311.

Kim, H. I. (2022) 'Efficient Deep Learning Network with Multi-Streams for Android Malware Family Classification', *IEEE Access*, 10, pp. 5518–5532. doi: 10.1109/ACCESS.2021.3139334.

Lakshmanarao, A. and Shashi, M. (2022) 'Android Malware Detection with Deep Learning using RNN from Opcode Sequences.', *International Journal of ...*. search.ebscohost.com. Available at: https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=18657923&AN=154752078&h=xxflScSbFqJ8QMBomebrlDj3Fs0fqgUaKFUbZN3guRKdm16MyiD7mVIJ0mNbFXtJMjjsYyJucNe5aOzPCbCZ4A%3D%3D&crl=c.

Liu, Y. (2019) 'Call Graph Based Android Malware Detection with CNN', *Communications in Computer and Information Science*, pp. 72–82. doi: 10.1007/978-981-15-0310-8_5.

Mercaldo, F. *et al.* (2022) 'Towards Explainable Quantum Machine Learning for Mobile Malware Detection and Classification †', *Applied Sciences (Switzerland)*, 12(23). doi: 10.3390/app122312025.

Muchlinski, D. (2022) 'Machine learning and deep learning', *Elgar Encyclopedia of Technology and Politics*. Electronic Markets, pp. 114–118. doi: 10.4337/9781800374263.machine.learning.deep.

Ning, B. (2021) 'Analysis of the Latest Trojans on Android Operating System', (January).

Pektaş, A. (2020) 'Deep learning for effective Android malware detection using API call graph embeddings', *Soft Computing*, 24(2), pp. 1027–1043. doi: 10.1007/s00500-019-03940-5.

Pektaş, A. and Acarman, T. (2020) 'Deep learning for effective Android malware

detection using API call graph embeddings', *Soft Computing*, 24(2), pp. 1027–1043. doi: 10.1007/s00500-019-03940-5.

Ren, Z. *et al.* (2020) 'End-to-end malware detection for android IoT devices using deep learning', *Ad Hoc Networks*. Elsevier B.V., 101, p. 102098. doi: 10.1016/j.adhoc.2020.102098.

Security, C., Nigussie, E. and Hakkala, A. (2021) 'Network Intrusion Detection System using Deep Learning Technique Title: Network Intrusion Detection System using Deep Learning Technique Number of pages: 75 pages, 2 appendix pages', (June).

Sharma, T. and Rattan, D. (2021) 'Malicious application detection in android - A systematic literature review', *Computer Science Review*. Elsevier Inc., 40, p. 100373. doi: 10.1016/j.cosrev.2021.100373.

Stiawan, D. *et al.* (2023) 'An Improved LSTM-PCA Ensemble Classifier for SQL Injection and XSS Attack Detection', *Computer Systems Science and Engineering*, 46(2), pp. 1759–1774. doi: 10.32604/csse.2023.034047.

Talal, M. *et al.* (2019) *Comprehensive review and analysis of anti-malware apps for smartphones*, *Telecommunication Systems*. Springer US. doi: 10.1007/s11235-019-00575-7.

Wang, Z. (2020) 'Review of android malware detection based on deep learning', *IEEE Access*, pp. 181102–181126. doi: 10.1109/ACCESS.2020.3028370.

Waterson, D. (2020) 'Managing endpoints, the weakest link in the security chain', *Network Security*. Elsevier Ltd, 2020(8), pp. 9–13. doi: 10.1016/S1353-4858(20)30093-3.

Wenbo, F. (2020) 'AMC-MDL: A Novel Approach of Android Malware Classification using Multimodel Deep Learning', *Proceedings - IEEE 18th International Conference on Dependable, Autonomic and Secure Computing, IEEE 18th International Conference on Pervasive Intelligence and Computing, IEEE 6th International Conference on Cloud and Big Data Computing and IEEE 5th Cybe*, pp. 251–256. doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00052.

Yadav, P. *et al.* (2022) 'A two-stage deep learning framework for image-based android malware detection and variant classification', *Computational …*. Wiley Online *Library*. doi: 10.1111/coin.12532.