

**Rancang Bangun Sistem Deteksi Adware Android Berbasis Web
Menggunakan XGBoost**



SKRIPSI

*diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana
Teknik pada Program Studi Teknik Komputer*

Oleh:

Afif Nasrullah Subagja

NIM 2102986

**PROGRAM STUDI S1 TEKNIK KOMPUTER
UNIVERSITAS PENDIDIKAN INDONESIA
KAMPUS UPI DI CIBIRU
2025**

HALAMAN HAK CIPTA

Rancang Bangun Sistem Deteksi Adware Android Berbasis Web Menggunakan XGBoost

Oleh
Afif Nasrullah Subagja
2102986

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Pendidikan pada Program Studi Teknik Komputer

© Afif Nasrullah Subagja 2025

Universitas Pendidikan Indonesia

15 Agustus 2025

Hak Cipta dilindungi undang-undang.

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,
dengan dicetak ulang, difotokopi, atau cara lainnya tanpa ijin dari penulis.

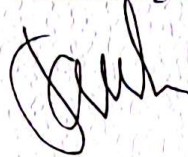
HALAMAN PENGESAHAN SKRIPSI

AFIF NASRULLAH SUBAGJA

Rancang Bangun Sistem Deteksi Adware Android Berbasis Web Menggunakan XGBoost

Disetujui dan disahkan oleh pembimbing:

Pembimbing 1



Muhammad Taufik, S.Tr.Kom., M.T.I.

NIP. 920200819940117101

Pembimbing 2



Nurhidayatulloh, S.Pd., M.T.

NIP. 920230219890404101

Mengetahui

Ketua Program Studi S-1 Teknik Komputer



Dr. Eng. Munawir, S.Kom., M.T.

NIP. 920200819851205101

ii

PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Afif Nasrullah Subagja

NIM : 2102986

Program Studi : Teknik Komputer

Judul Karya : Rancang Bangun Sistem Deteksi Adware Android Berbasis Web
Menggunakan XGBoost

Dengan ini menyatakan bahwa karya tulis ini merupakan hasil kerja saya sendiri. Saya menjamin bahwa seluruh isi karya ini, baik sebagian maupun keseluruhan, bukan merupakan plagiarisme dari karya orang lain, kecuali pada bagian yang telah dinyatakan dan disebutkan sumbernya dengan jelas.

Jika di kemudian hari ditemukan pelanggaran terhadap etika akademik atau unsur plagiarisme, saya bersedia menerima sanksi sesuai peraturan yang berlaku di Universitas Pendidikan Indonesia.

Kabupaten Bandung, 15 Agustus 2025



Afif Nasrullah Subagja

KATA PENGANTAR

Dengan penuh rasa syukur kepada Allah SWT atas rahmat dan karunia-Nya, penulis dapat menyelesaikan skripsi yang berjudul " Rancang Bangun Sistem Deteksi Adware Android Berbasis Web Menggunakan XGBoost" Skripsi ini diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik (S.T) pada Program Studi Teknik Komputer, Kampus UPI di Cibiru, Universitas Pendidikan Indonesia.

Penelitian ini dapat diselesaikan dengan sebaik-baiknya berkat dukungan, bantuan, serta doa dari berbagai pihak. Oleh karena itu, dengan segala hormat dan rasa terima kasih yang tulus, penulis menyampaikan penghargaan sebesar-besarnya kepada:

1. Bapak Muhammad Taufik, S.Tr.Kom., M.T.I., selaku Pembimbing I sekaligus Kepala Program Studi, yang dengan penuh kesabaran telah memberikan bimbingan, ilmu, serta arahan yang sangat berharga selama proses penelitian ini, serta dukungan dalam menghadapi berbagai tantangan selama perkuliahan.
2. Bapak Nurhidayatulloh, S.Pd., M.T., selaku Pembimbing II, atas segala bimbingan, nasihat, dan dukungan yang diberikan baik dalam penyusunan skripsi maupun selama masa studi.
3. Bapak Dr. Eng. Munawir, S.Kom., M.T. dan Ibu Ana Rahma Yuniarti, S.T., M.Eng., selaku Dosen Pembimbing Akademik, atas segala bimbingan, arahan, dan dukungan yang senantiasa diberikan selama masa perkuliahan hingga proses penyusunan skripsi ini.
4. Bapak Wahyu Setiawan, selaku staf Program Studi, atas segala bantuan, nasihat, dan arahan yang diberikan selama masa perkuliahan.
5. Seluruh *civitas* akademika UPI Kampus Cibiru, khususnya para dosen dan staf yang telah memberikan ilmu, arahan, serta fasilitas yang mendukung kelancaran studi dan penelitian ini.

6. Rekan-rekan mahasiswa Teknik Komputer, yang telah menjadi teman seperjuangan selama masa studi, berbagi ilmu, pengalaman, serta semangat dalam menghadapi berbagai tantangan akademik.
7. Kedua orang tua, yang senantiasa memberikan kasih sayang, doa, dukungan moral, serta materi yang tak terhingga nilainya. Tanpa restu dan doa mereka, penulis tidak akan bisa mencapai tahap ini. Semua yang telah penulis capai hingga saat ini adalah berkat dukungan serta pengorbanan mereka.
8. Semua pihak yang telah membantu, baik secara langsung maupun tidak langsung, yang namanya tidak dapat disebutkan satu per satu, namun telah memberikan dukungan, semangat, serta inspirasi dalam menyelesaikan skripsi ini. Setiap bantuan yang diberikan sangat berarti bagi penulis.

Rancang Bangun Sistem Deteksi Adware Android Berbasis Web Menggunakan XGBoost

Afif Nasrullah Subagja

2102986

ABSTRAK

Pertumbuhan pesat sistem operasi Android di seluruh dunia, termasuk di Indonesia, yang meningkat dari 54 juta pengguna pada 2015 menjadi 209,3 juta pada 2023, menghadirkan peluang sekaligus tantangan dalam keamanan siber. Salah satu tantangan besar adalah adware, yang menampilkan iklan agresif dan berpotensi mencuri data pribadi. Penelitian ini bertujuan membangun sistem deteksi adware pada aplikasi Android berbasis web menggunakan model XGBoost untuk mengklasifikasikan file APK menjadi *Benign* (aman) dan Adware (berbahaya), dengan pendekatan *Design and Development* (D&D) meliputi eksplorasi masalah, pengembangan model, perancangan sistem, dan evaluasi, serta pembangunan website menggunakan HTML, CSS, dan Bootstrap untuk antarmuka pengguna dengan Flask sebagai backend. Pengujian pada 124 file APK asli menunjukkan akurasi 96,77% dengan sebagian besar file terklasifikasi benar. Implementasi sistem berbasis web menampilkan antarmuka sederhana dan mudah digunakan, menyajikan hasil prediksi secara jelas, serta memberikan pendekatan yang tepat untuk meningkatkan keamanan aplikasi Android dan kesadaran pengguna terhadap adware. Model *machine learning* berbasis XGBoost berhasil diimplementasikan ke dalam aplikasi berbasis web dan mampu mendeteksi adware dengan tingkat kesalahan yang sangat rendah.

Kata Kunci: Android, Adware, Keamanan Siber, XGBoost

Design and Development of a Web-Based Android Adware Detection System Using XGBoost

Afif Nasrullah Subagja

2102986

ABSTRACT

The rapid growth of the Android operating system worldwide, including in Indonesia, which increased from 54 million users in 2015 to 209.3 million in 2023, presents both opportunities and challenges in cybersecurity. One of the major challenges is adware, which displays aggressive advertisements and has the potential to steal personal data. This research aims to develop an adware detection system for Android applications based on a web platform, utilizing the XGBoost model to classify APK files into Benign (safe) and Adware (malicious) categories. The study employs the Design and Development (D&D) approach, which includes problem exploration, model development, system design, and evaluation, along with the development of a website using HTML, CSS, and Bootstrap for the user interface and Flask as the backend. Testing on 124 original APK files achieved an accuracy of 96.77%, with the majority of files correctly classified. The implementation of the web-based system provides a simple and user-friendly interface, clearly presents prediction results, and offers an effective approach to enhancing Android application security and user awareness of adware. The machine learning model based on XGBoost was successfully implemented into the web application and is capable of detecting adware with a very low error rate.

Keywords: Android, Adware, Cybersecurity, XGBoost

DAFTAR ISI

HALAMAN HAK CIPTA	i
HALAMAN PENGESAHAN SKRIPSI.....	ii
PERNYATAAN BEBAS PLAGIARISME	iii
KATA PENGANTAR.....	iv
ABSTRAK	vi
<i>ABSTRACT</i>	vii
DAFTAR ISI	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
DAFTAR PERSAMAAN	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Penelitian	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian.....	3
1.5 Ruang Lingkup Penelitian	4
BAB II TINJAUAN PUSTAKA	5
2.1 Android.....	5
2.1.1 Riwayat Versi Android.....	7
2.1.2 Arsitektur Sistem Operasi Android.....	8
2.2 Adware	11
2.2.1 Adware Android.....	12

2.2.2 Jenis-jenis Adware	13
2.3 <i>Machine Learning</i>	16
2.4 XGBoost.....	18
2.5 Website	19
2.6 Penelitian Terdahulu	19
BAB III METODE PENELITIAN.....	22
3.1 Eksplorasi dan Identifikasi Masalah.....	22
3.2 Perancangan Sistem.....	23
3.2.1 Perancangan Model.....	23
3.2.1.1 Data Scoping	24
3.2.1.2 Data Acquisition.....	24
3.2.1.3 Data Exploration	25
3.2.1.4 Modelling	25
3.2.1.5 Model Evaluation	25
3.2.2 Perancangan Aplikasi.....	26
3.1.3.1 Use Case Diagram.....	26
3.1.3.2 Activity Diagram.....	28
3.1.3.3 Flowchart Sistem.....	30
3.1.3.4 Mockup Antarmuka.....	32
3.3 Pengembangan Sistem.....	33
3.3.1 Tahap Communication	34
3.3.2 Tahap Quick Plan	34
3.3.3 Tahap Construction of Prototype.....	35
3.3.4 Tahap Communication	35
3.4 Evaluasi Sistem	36

3.4.1 Pengujian Model	36
3.4.1 Pengujian Aplikasi	37
BAB IV HASIL DAN PEMBAHASAN.....	39
4.1 Hasil Perancangan Model.....	39
4.2 Hasil Pengujian Model	41
4.3 Hasil Perancangan Aplikasi.....	43
4.3.1 Antarmuka Pengguna	43
4.3.2 Fitur Aplikasi	45
4.4 Hasil Pengujian Aplikasi	46
BAB V SIMPULAN DAN SARAN	49
5.1 Simpulan.....	49
5.2 Saran	49
DAFTAR PUSTAKA	51
LAMPIRAN.....	55

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu.....	21
Tabel 4. 1 Distribusi File APK Pengujian	42
Tabel 4. 3 Pengujian Fungsional Website	47

DAFTAR GAMBAR

Gambar 2.1 Perbandingan Kinerja Dalvik dan ART	9
Gambar 2. 2 Arsitektur Android.....	9
Gambar 2.3 Lapisan Kernel.....	10
Gambar 2.4 Lapisan Libraries.....	10
Gambar 2.5 Teknik Umum untuk Penipuan Iklan.....	13
Gambar 3.1 Tahapan Penelitian	22
Gambar 3. 2 Metode Pengembangan AI Project Cycle	24
Gambar 3. 3 Use Case Diagram Sistem Deteksi Adware	27
Gambar 3. 4 Activity Diagram Sistem Deteksi Adware	29
Gambar 3. 5 Flowchart Sistem Deteksi Adware	31
Gambar 3. 6 Mockup Antarmuka.....	33
Gambar 4. 1 Kode Pelatihan Model XGBoost.....	39
Gambar 4. 2 Perfoma Model XGBoost.....	40
Gambar 4. 3 Confusion Matrix	40
Gambar 4. 4 Grafik Training vs Validation XGBoost.....	41
Gambar 4. 5 Confusion Matrix Pengujian	42
Gambar 4. 6 Tampilan Homepage.....	43
Gambar 4. 7 Tampilan Upload page.....	44
Gambar 4. 8 Tampilan Hasil Prediksi	44
Gambar 4. 9 Notifikasi validasi ukuran	45
Gambar 4. 10 Hasil Ekstraksi Fitur.....	45
Gambar 4. 11 Hasil Klasifikasi Model.....	46
Gambar 4. 12 Ringkasan Klasifikasi dan Keakuratan	46

DAFTAR PERSAMAAN

Persamaan <i>Accuracy</i> (1).....	37
Persamaan <i>Precision</i> (2).....	37
Persamaan <i>Recall</i> (3).....	37
Persamaan <i>F1-Score</i> (4)	37

DAFTAR LAMPIRAN

Lampiran 1 Jadwal Penelitian	55
Lampiran 2 Tampilan Web	55
Lampiran 3 Struktur File	61
Lampiran 4 Code Flask	62
Lampiran 5 Code XGBoost	62
Lampiran 6 Hasil Pengujian	63
Lampiran 7 Hasil Pengujian Similarity	68
Lampiran 8 Hasil Pengujian Deteksi AI	68

DAFTAR PUSTAKA

- [1] H. AlOmari, Q. M. Yaseen, and M. A. Al-Betar, "A Comparative Analysis of Machine Learning Algorithms for Android Malware Detection," *Procedia Comput. Sci.*, vol. 220, pp. 763–768, 2023, doi: 10.1016/j.procs.2023.03.101.
- [2] M. Syaharani, "10 Negara Dengan Pengguna Smartphone Terbanyak Di Dunia, Indonesia Masuk Daftar!," *GoodStats*, Agustus 2023. Accessed: Apr. 12, 2025. [Online]. Available: <https://goodstats.id/article/10-negara-dengan-pengguna-smartphone-terbanyak-di-dunia-indonesia-masuk-daftar-fDv25>
- [3] S. F. T. Andalas, "209,3 Juta Orang di Indonesia Menggunakan Smartphone pada Tahun 2023," *GoodStats*, Jun. 12, 2024. Accessed: Apr. 12, 2025. [Online]. Available: <https://data.goodstats.id/statistic/2093-juta-orang-di-indonesia-menggunakan-smartphone-pada-tahun-2023-cbha0>
- [4] M. M. Alani and A. I. Awad, "AdStop: Efficient flow-based mobile adware detection using machine learning," *Comput. Secur.*, vol. 117, p. 102718, Jun. 2022, doi: 10.1016/j.cose.2022.102718.
- [5] D. Novianty, "Serangan Adware Mendominasi Perangkat Seluler di Sepanjang 2023," *suara.com*, Mar. 03, 2024. Accessed: Apr. 12, 2025. [Online]. Available: <https://www.suara.com/tekno/2024/03/03/165949/serangan-adware-mendominasi-perangkat-seluler-di-sepanjang-2023>
- [6] S. Suresh, F. Di Troia, K. Potika, and M. Stamp, "An analysis of Android adware," *J. Comput. Virol. Hacking Tech.*, vol. 15, no. 3, pp. 147–160, Sep. 2019, doi: 10.1007/s11416-018-0328-8.
- [7] A. Tanujaya, "Malware Indonesia Q4 - 2023," *vaksin.com*, Dec. 30, 2023. Accessed: Apr. 12, 2025. [Online]. Available: <https://www.vaksin.com/malware-indonesia-q4-2023>
- [8] M. H. Arief, K. A. Fitri, and E. M. Sari, "Analisis Kesadaran Cyber Crime Di Kalangan Masyarakat Menengah Kebawah," *Tekinfo*, vol. 22, no. 2, 2024, doi: 10.37817/tekinfo.v25i2.
- [9] N. Vadila and A. R. Pratama, "Analisis Kesadaran Keamanan Terhadap Ancaman Phishing," *ETHOS Jurnal Penelitian dan Pengabdian*, vol. 7, no. 1, pp. 9–17, Jan. 2019, doi: 10.29313/ethos.v7i1.3850.
- [10] I. A. Saputro, L. Sugiarto, and F. S. Nugraha, "Analisis Kesadaran Masyarakat Terhadap Bahaya Internet Phishing Menggunakan K-Means Clustering," *STRING Satuan Tulisan Riset dan Inovasi Teknologi*, vol. 9, no. 2, p. 139, Dec. 2024, doi: 10.30998/string.v9i2.22404.

- [11] R. Akraman, C. Candiwan, and Y. Priyadi, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia," *J. Sist. Inf. BISNIS*, vol. 8, no. 2, p. 115, Oct. 2018, doi: 10.21456/vol8iss2pp115-122.
- [12] C. Li, K. Mills, R. Zhu, D. Niu, H. Zhang, and H. Kinawi, "Android Malware Detection based on Factorization Machine," *IEEE*, Aug. 13, 2019, *arXiv*: arXiv:1805.11843. doi: 10.48550/arXiv.1805.11843.
- [13] Ansumana F Jadama, Modou K Toray, A. Sami, and Rohith Kumar Saravanan, "Classification of Mobile Adware Variants Using Machine Learning Techniques," *ResearchGate*, 2024, doi: 10.13140/RG.2.2.15406.83522.
- [14] O. Sh. A. Aboosh and O. A. I. Aldabbagh, "Android Adware Detection Model Based on Machine Learning Techniques," in *2021 International Conference on Computing and Communications Applications and Technologies (I3CAT)*, Ipswich, United Kingdom: IEEE, Sep. 2021, pp. 98–104. doi: 10.1109/I3CAT53310.2021.9629400.
- [15] W. Jobe, "Native Apps Vs. Mobile Web Apps," *Int. J. Interact. Mob. Technol. IJIM*, vol. 7, no. 4, p. 27, Oct. 2013, doi: 10.3991/ijim.v7i4.3226.
- [16] S. Patil, "Progressive Web Apps (Pwas) Vs. Native Apps: a Technical and UX Comparison," *IJIRT*, vol. 12, no. 1, 2025.
- [17] B. Malle, N. Giuliani, P. Kieseberg, and A. Holzinger, "The Need for Speed of AI Applications: Performance Comparison of Native vs. Browser-based Algorithm Implementations," *ResearchGate*, Feb. 11, 2018, *arXiv*: 1802.03707. doi: 10.48550/.
- [18] Yun Ma, Xuanzhe Liu, Yi Liu, Yunxin Liu, and Gang Huang, "A Tale of Two Fashions: An Empirical Study on the Performance of Native Apps and Web Apps on Android," *IEEE Trans. Mob. Comput.*, vol. 17, no. 5, 01 May 2018), pp. 990–1003, Sep. 2017, doi: 10.1109/TMC.2017.2756633.
- [19] Kirthika.B, Prabhu.S, and Visalakshi.S, "Android Operating System: A Review," *Int. J. Trend Res. Dev.*, 2015, [Online]. Available: <https://www.ijtrd.com/>
- [20] Amity School of Engineering and technology, Amity University, Lucknow, India, A. Tewari, P. Singh, and Amity School of Engineering and technology, Amity University, Lucknow, India, "Android App Development: A Review," *J. Manag. Serv. Sci. JMSS*, vol. 1, no. 2, pp. 1–6, Aug. 2021, doi: 10.54060/JMSS/001.02.006.
- [21] N. Ekanayaka, "Android Operating System," *ResearchGate*, 2018.

- [22] Iggy Krajci and Darren Cummings, " *Android on x86: an Introduction to Optimizing for Intel® Architecture*," Apress, 2014.
- [23] Yudhistira, "Urutan Versi Android dari Awal Hingga Android 15," *Bhinneka*, Sep. 08, 2024. Accessed: Apr. 16, 2025. [Online]. Available: <https://www.bhinneka.com/blog/urutan-android/>
- [24] P. Gilski and J. Stefanski, "Android OS: A Review," *TEM J.*, pp. 116–120, Feb. 2015, doi: 10.18421/TEM41-14.
- [25] M. Jaiswal, "Android The Mobile Operating System And Architecture," *ResearchGate*, vol. 6, no. 1, 2018.
- [26] Seyhmus Yilmaz and Sultan Zavrak, "Adware: A Review," *IJCSIT Int. J. Comput. Sci. Inf. Technol.*, vol. Vol. 6 (6), 2015, [Online]. Available: https://www.researchgate.net/publication/294709236_Adware_A_Review?enrichId=rgreq-7ae324acf482c943562c916384ff1d5d-XXX&enrichSource=Y292ZXJQYWdlOzI5NDcwOTIzNjBUzozMjk3MjQzNDY4MTQ0NjRAMTQ1NTYyMzgxODU3Mg%3D%3D&el=1_x_2&_esc=publicationCoverPdf
- [27] S. Seraj, M. Pavlidis, M. Trovati, and N. Polatidis, "MadDroid: malicious adware detection in Android using deep learning," *J. Cyber Secur. Technol.*, vol. 8, no. 3, pp. 163–190, Jul. 2024, doi: 10.1080/23742917.2023.2247197.
- [28] K. Das, R. N. Behera, and B. Tech, "A Survey on Machine Learning: Concept, Algorithms and Applications," *ResearchGate*, vol. 5, no. 2, 2007.
- [29] D. M. Abdulqader, A. M. Abdulazeez, and D. Q. Zeebaree, "Machine Learning Supervised Algorithms of Gene Selection: A Review," *ResearchGate*, vol. 62, no. 03, 2020.
- [30] Z. Arif Ali, Z. H. Abduljabbar, H. A. Tahir, A. Bibo Sallow, and S. M. Almufti, "eXtreme Gradient Boosting Algorithm with Machine Learning: a Review," *Acad. J. Nawroz Univ.*, vol. 12, no. 2, pp. 320–334, May 2023, doi: 10.25007/ajnu.v12n2a1612.
- [31] C. Bentejac, A. Csorgo, and G. Martinez-Munoz, "A Comparative Analysis of XGBoost," *ResearchGate*, 2019, doi: 10.48550/arXiv.1911.01914.
- [32] D. Chaudhary, K. Bakshi, and P. K. Jha, "Detection of Malware and Adware Using Machine Learning: A Practical Approach," *ResearchSquare* Apr. 10, 2024. doi: 10.21203/rs.3.rs-4219382/v1.
- [33] R. C. Richey and J. D. Klein, " *Design and Development Research: Methods, Strategies, and Issues*," Hoboken: Taylor and Francis, 2007.

- [34] C. A. Aurelia and D. A. Prasetya, “Implementasi Pembelajaran AI Mastery Program dalam Mengembangkan Aplikasi Berbasis Web di PT. Orbit Ventura Indonesia,” *Soc. J. Pengabd. Dan Pemberdaya. Masy.*, vol. 4, no. 1, pp. 1–10, Oct. 2023, doi: 10.37802/society.v4i1.299.
- [35] T. Pricillia and Zulfachmi, “Perbandingan Metode Pengembangan Perangkat Lunak (Waterfall, Prototype, RAD),” *J. Bangkit Indones.*, vol. 10, no. 1, pp. 6–12, Mar. 2021, doi: 10.52771/bangkitindonesia.v10i1.153.
- [36] M. Alda, M. Alfari, A. B. Barus, I. Syahfitri, and A. Asnawi, “Perancangan Aplikasi Digital Perpustakaan Menggunakan Metode Prototyping Berbasis Android,” *Innov. J. Soc. Sci. Res.*, vol. Volume 4 Nomor 1 Tahun 2024 Page 8143-8153, 2024.
- [37] K. Wijaya and A. Christian, “Implementasi Metode Model View Controller (MVC) Dalam Rancang Bangun Website SMK Yayasan Bakti Prabumulih,” *Paradig. - J. Komput. Dan Inform.*, vol. 21, no. 1, pp. 95–102, Mar. 2019, doi: 10.31294/p.v21i1.5092.