MENINGKATKAN DETEKSI MALWARE BERBASIS MACHINE LEARNING MELALUI PENGURANGAN FITUR BERBASIS IQR

SKRIPSI NON REGULER - SCIENTIST

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

Nurcahyo Fajar Setyanto

21.83.0676

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

MENINGKATKAN DETEKSI MALWARE BERBASIS MACHINE LEARNING MELALUI PENGURANGAN FITUR BERBASIS IQR

SKRIPSI NON REGULER - SCIENTIST

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

Nurcahyo Fajar setyanto

21.83.0676

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI NON REGULER – SCIENTIST

MENINGKATKAN DETEKSI MALWARE BERBASIS MACHINE LEARNING MELALUI PENGURANGAN FITUR BERBASIS IQR

yang disusun dan diajukan oleh

Nurcahyo Fajar Setyanto

21.83.0676

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 07 Januari 2026

Dosen Pembimbing,

Rina Pramitasari, S.Si., M.Cs.
NIK. 190302096

HALAMAN PENGESAHAN

SKRIPSI NON REGULER - SCIENTIST

MENINGKATKAN DETEKSI MALWARE BERBASIS MACHINE LEARNING MELALUI PENGURANGAN FITUR BERBASIS IQR

yang disusun dan diajukan oleh

Nurcahyo Fajar Setyanto

21.83.0676

Telah dipertahankan di depan Dewan Penguji
pada tanggal 19 Februari 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Andika Agus Slameto, S.Kom., M.Kom. **NIK. 190302109**	
Muhammad Koprawi, S.Kom., M.Eng. **NIK. 190302454**	
Rina Pramitasari, S.Si., M.Cs. **NIK. 190302096**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Februari 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Nurcahyo Fajar Setyanto
NIM : 21.83.0676

Menyatakan bahwa Skripsi dengan judul berikut:

Meningkatkan Deteksi Malware Berbasis Machine Learning Melalui Pengurangan Fitur Berbasis IQR
Dosen Pembimbing : Rina Pramitasari, S.Si., M.Cs

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 19 Februari 2026

Yang Menyatakan,

Nurcahyo Fajar Setyanto

HALAMAN PERSEMBAHAN

Segala puji dan syukur penulis panjatkan ke hadirat Allah Subhanahu wa Ta'ala atas segala limpahan rahmat, petunjuk, dan kekuatan yang diberikan selama proses penulisan skripsi ini. Dengan penuh rasa hormat dan cinta, penulis mempersembahkan karya sederhana ini kepada:

- Tugiman dan Purnawati, orang tua tercinta, yang menjadi sumber kekuatan dan semangat dalam setiap langkah hidup penulis. Terima kasih atas cinta yang tulus, doa yang tak pernah putus, serta dukungan tanpa syarat, baik secara moral maupun materiil. Pencapaian ini tidak akan pernah terwujud tanpa kalian.
- Rezky Akbar Nur Faizal selaku adik penulis yang telah memberikan bantuan saat mengerjakan skripsi ataupun bantuan saat menjalani kuliah
- Seluruh keluarga besar, yang senantiasa memberikan dorongan, kepercayaan, dan doa yang menguatkan. Kehadiran kalian menjadi energi positif yang memotivasi penulis untuk menyelesaikan tanggung jawab akademik ini.
- Teman-teman Heyek Gank yang tidak bisa saya sebut satu persatu. Terima kasih atas segala kebersamaan, tawa, kerja sama, dan semangat yang tak pernah padam.
- Seluruh pihak yang turut membantu, baik secara langsung maupun tidak langsung, dalam bentuk bimbingan, motivasi, maupun dukungan lainnya selama proses studi dan penyusunan skripsi ini.

Skripsi ini merupakan hasil dari proses panjang yang penuh tantangan, doa, dan pengorbanan. Semoga karya ini dapat memberikan manfaat dan menjadi langkah awal untuk pengabdian yang lebih luas di masa depan.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas berkat rahmat dan karunia-Nya, penulis dapat menyelesaikan skripsi ini dengan judul "Meningkatkan Deteksi Malware Berbasis Machine Learning Melalui Pengurangan Fitur Berbasis IQR" sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Teknik Komputer di Universitas Amikom Yogyakarta.

Penulisan skripsi ini tidak lepas dari bimbingan, dukungan, dan bantuan berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

- Orang tua tercinta yang selalu memberikan doa, dukungan, dan kasih sayang yang tiada henti.
- Dosen pembimbing yang telah memberikan arahan, bimbingan, serta motivasi yang luar biasa selama proses penyusunan skripsi ini.
- Seluruh dosen dan staf akademik di lingkungan Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.
- Teman-teman Heyek Gank, yang telah memberikan dukungan moral, motivasi, dan kerja sama selama ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna, baik dari segi isi maupun penyusunannya. Oleh karena itu, penulis mengharapkan kritik dan saran yang konstruktif demi perbaikan dan pengembangan pengetahuan di masa depan. Semoga skripsi ini dapat memberikan kontribusi yang bermanfaat bagi perkembangan ilmu pengetahuan, khususnya di bidang cyber security.

Akhir kata, penulis berharap semoga skripsi ini dapat bermanfaat bagi para pembaca, terutama dalam praktis di bidang cyber security.

Yogyakarta, 07 Januari 2026

Penulis,

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

INTISARI

Deteksi malware merupakan tantangan signifikan dalam keamanan siber karena sifat ancaman yang kompleks dan terus berkembang. Studi ini mengevaluasi efektivitas algoritma pembelajaran mesin, khususnya XGBoost dan LightGBM, dalam mendeteksi malware. Pendekatan ini mencakup pembersihan data, normalisasi, pemilihan fitur, dan penggunaan teknik Interquartile Range (IQR) untuk memilih fitur yang relevan. Set data awal berisi 21.752 berkas, yang terbagi rata antara berkas berbahaya dan tidak berbahaya, dengan banyak fitur yang berkurang setelah menerapkan IQR. Hasil menunjukkan bahwa XGBoost mengungguli algoritma lain, mencapai akurasi 99,20%, sebuah peningkatan dibandingkan akurasi 98,99% tanpa IQR. Teknik IQR meningkatkan kualitas data dengan memfilter fitur-fitur yang memiliki perbedaan signifikan antara malware dan berkas tidak berbahaya, sehingga meningkatkan kinerja model. Selain itu, pengurangan set fitur membantu mencegah overfitting dan memperkuat kemampuan generalisasi model. Studi ini menyimpulkan bahwa pembelajaran mesin, khususnya dengan algoritma seperti XGBoost dan LightGBM, dapat secara efektif meningkatkan deteksi malware. Dengan menggunakan IQR dalam pemilihan fitur, kinerja model ditingkatkan, sehingga mengurangi positif palsu dan meningkatkan efisiensi deteksi. Penelitian ini menyoroti pentingnya teknik pemilihan fitur seperti IQR dalam meningkatkan daya prediktif model pembelajaran mesin, sehingga lebih efisien dalam mengidentifikasi malware. Penelitian selanjutnya akan mengeksplorasi metode pemilihan fitur tambahan untuk lebih meningkatkan akurasi deteksi malware.

Kata kunci: Malware, Machine Learning, Interquartile Range, XGBoost, Deteksi Malware

ABSTRACT

Malware detection is a significant challenge in cybersecurity due to the complex and evolving nature of threats. This study evaluates the effectiveness of machine learning algorithms, specifically XGBoost and LightGBM, in detecting malware. The approach includes data cleaning, normalization, feature selection, and the use of the Interquartile Range (IQR) technique to select relevant features. The initial dataset contained 21,752 files, evenly split between malicious and benign files. After data cleaning, the number of samples decreased to 19,256 files, with numerous features that were reduced after applying IQR. Results show that XGBoost outperforms other algorithms, achieving 99.20% accuracy, an improvement over the 98.99% accuracy without IQR. The IQR technique enhances data quality by filtering out features with significant differences between malware and benign files, improving model performance. Additionally, reducing the feature set helps prevent overfitting and strengthens the model's generalization ability. The study concludes that machine learning, particularly with algorithms like XGBoost and LightGBM, can effectively improve malware detection. By using IQR in feature selection, model performance is enhanced, leading to reduced false positives and increased detection efficiency. The research highlights the importance of feature selection techniques like IQR in boosting the predictive power of machine learning models, making them more efficient in identifying malware. Future work will explore additional feature selection methods to further improve malware detection accuracy.

Keyword: *Malware, Machine Learning, Interquartile Range, XGBoost, Malware Detection*