DETEKSI RANSOMWARE BERBASIS PERILAKU (*BEHAVIOUR-BASED*) DENGAN PENDEKATAN DEEP LEARNING

SKRIPSI

Benaya Adi Sahat Dwiyanto

2107412033

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Teknik

PROGRAM STUDI TEKNIK INFORMATIKA

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

TAHUN 2025/2026

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini:

Nama	: Benaya Adi Sahat Dwiyanto
NIM	: 2107412033
Jurusan/Program Studi	: T. Informatika dan Komputer/Teknik Informatika
Judul Skripsi	: DETEKSI RANSOMWARE BERBASIS PERILAKU (*BEHAVIOUR-BASED*) DENGAN PENDEKATAN DEEP LEARNING

Menyatakan dengan sebenarnya bahwa skripsi ini benar benar merupakan hasil karya saya sendiri bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 19 Juni 2025

Yang membuat pernyataan

Benaya Adi Sahat Dwiyanto

NIM 2107412033

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama : Benaya Adi Sahat Dwiyanto
NIM : 2107412033
Program Studi : Teknik Informatika
Judul Skripsi : DETEKSI RANSOMWARE BERBASIS PERILAKU (BEHAVIOUR-BASED) DENGAN PENDEKATAN DEEP LEARNING

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Jumat, Tanggal 5 Bulan Juli, Tahun 2025 dan dinyatakan LULUS.

Disahkan oleh :

Pembimbing I : Dr. Dewi Yanti Liliana, S.Kom., M.Kom. (.....)

Penguji I : Mera Kartika Delimayanti, S.Si., M.T., Ph.D (.....)

Penguji II : Rizki Elisa Nalawati, S.T.,M.T. (.....)

Penguji III : Bambang Warsuta, S.Kom, M.T.I (.....)

Mengetahui:
Jurusan Teknik Informatika dan Komputer
Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh, Shalom, Puji Syukur kepada Tuhan penulis panjatkan kepada Tuhan YME yang telah memberikan karunia dan anugerah-Nya kepada penulis sehingga penulis dapat menyelesaikan skripsi yang berjudul "DETEKSI RANSOMWARE BERBASIS PERILAKU (*BEHAVIOUR-BASED*) DENGAN PENDEKATAN DEEP LEARNING" sebagai salah satu persyaratan guna memperoleh gelar Sarjana Terapan Program Studi Teknik Informatika di Politeknik Negeri Jakarta.

Penulis sangat menyadari bahwa banyak pihak yang mendukung dan memberikan bantuan kepada penulis dari awal hingga tahap penyelesaian skripsi ini. Dengan demikian, penulis ingin berterima kasih yang sebesar-besarnya kepada pihak-pihak yang terlibat. Secara khusus, penulis menyampaikan ucapan terimakasih kepada :

1. Ibu Dr. Anita Hidayati, S. Kom., M. Kom., selaku Ketua Jurusan Teknik Informatika dan Komputer.
2. Ibu Euis Oktavianti, S.Si., M.TI., selaku Kepala Program Studi Teknik Informatika.
3. Ibu Dr. Dewi Yanti Liliana, S. Kom., M. Kom., selaku Dosen Pembimbing yang sudah bersedia meluangkan waktu untuk membantu, mengarahkan, serta menyemangati dalam proses penyelesaian skripsi ini.
4. Seluruh Bapak/Ibu dosen yang sudah mendidik penulis sehingga menjadi pribadi yang lebih baik.
5. Kedua orang tua penulis yang senantiasa selalu mendukung, mendoakan dan memberikan semangat serta kasih sayang kepada penulis dengan tiada henti-hentinya.
6. Teman-teman penulis yang selalu memberikan dukungan dan menemani penulis dalam proses penyelesaian skripsi ini.

Akhir kata, penulis berharap skripsi yang ditulis ini dapat memberikan manfaat kepada berbagai pihak, terutama di bidang keamanan siber. Penulis menyadari bahwa skripsi ini jauh dari kata sempurna, oleh karena itu, penulis mengharapkan

segala bentuk kritik, saran, dan masukan yang membangun yang dapat memperbaiki serta menyempurnakan skripsi ini.

Wassalamualaikum Warahmatullahi Wabarakatuh, Shalom

Depok, 19 Juni 2025

Benaya Adi Sahat Dwiyanto

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama : Benaya Adi Sahat Dwiyanto

NIM : 2107412033

Jurusan/Program Studi : T.Informatika dan Komputer/ T. Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Royalti Non-Eksklusif atas karya ilmiah say yang berjudul :

DETEKSI RANSOMWARE BERBASIS PERILAKU (*BEHAVIOUR-BASED*) DENGAN PENDEKATAN DEEP LEARNING

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalih mediakan /format kan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 24 Juli 2025

Yang membuat pernyataan

Benaya Adi Sahat Dwiyanto

NIM 2107412033

DETEKSI RANSOMWARE BERBASIS PERILAKU (*BEHAVIOUR-BASED*) DENGAN PENDEKATAN DEEP LEARNING

ABSTRAK

Seiring meningkatnya ancaman siber, khususnya ransomware yang semakin canggih, metode deteksi konvensional berbasis signature-based menjadi tidak lagi memadai. Penelitian ini mengembangkan sistem deteksi ransomware menggunakan pendekatan berbasis perilaku (behaviour-based) dengan menganalisis sekuens panggilan Application Programming Interface (API calls) yang diekstraksi melalui analisis dinamis dalam sandbox CAPEv2. Empat arsitektur deep learning, yaitu Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Bidirectional LSTM (Bi-LSTM), dan hibrida CNN-LSTM dibangun dan dievaluasi untuk mengklasifikasikan file .exe sebagai ransomware atau benign. Hasil pengujian pada set data uji terpisah menunjukkan bahwa model Bi-LSTM mencapai performa terbaik dengan akurasi 99.51%, yang secara signifikan mengungguli model LSTM standar (85.71%) dan CNN (51.72%). Hasil ini membuktikan bahwa kemampuan Bi-LSTM dalam memahami konteks sekuensial dari dua arah sangat efektif untuk mengidentifikasi pola perilaku ransomware. Sistem deteksi ini kemudian diimplementasikan ke dalam sebuah aplikasi web praktis untuk memvalidasi fungsionalitasnya dalam skenario penggunaan nyata.

Kata Kunci: Deteksi Ransomware, Behaviour-Based, Analisis Dinamis, API Calls, Deep Learning, CNN, LSTM, Bi-LSTM, Sandbox

DAFTAR PUSTAKA

DAFTAR TABEL

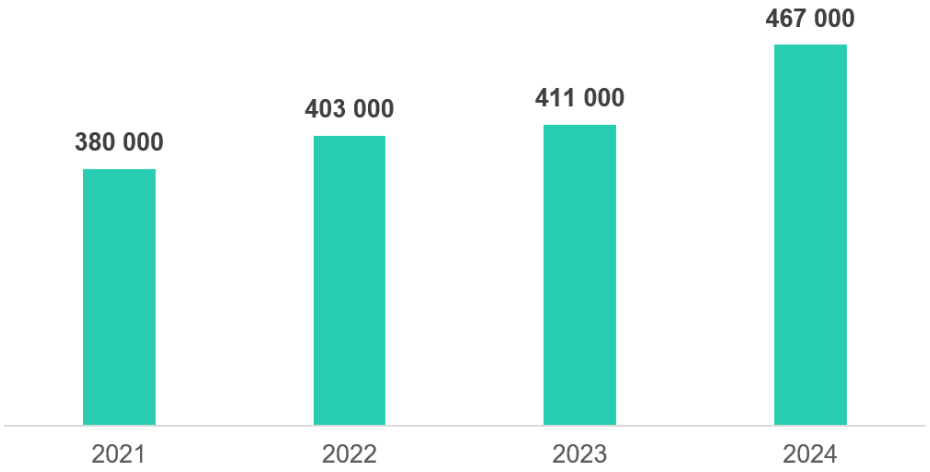
DAFTAR GAMBAR

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam dunia teknologi yang serba cepat dan dinamis, informasi menjadi salah satu bagian terpenting di dalamnya. Informasi sebagai aset yang sangat berharga karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha dan kepercayaan publik (Ramadhani, A. (2018)). Dan Internet, telah menjadi sumber informasi yang penting akhir-akhir ini (Azeem et al. 2024). Dilansir dari penelitian yang dilakukan oleh Kaspersky Labs, menunjukkan bahwa 44% pengguna internet membuat informasi mereka menjadi publik, dimana 37% membagikan rincian keuangan dan pembayaran, sebanyak 41% membagikan pemindaian paspor, SIM, dan dokumen pribadi lainnya, dan 30% membagikan kata sandi mereka (Kaspersky, 2017). Ini, menjadikan keamanan digital dalam menjaga informasi merupakan hal yang penting dan krusial, untuk menjaga data-data sensitif dari pihak pihak yang tidak bertanggung jawab, yang dapat menyalahgunakan data-data sensitif tersebut.

Serangan siber semakin menjadi kenyataan sehari-hari baik bagi perusahaan besar maupun perorangan, namun sedikit sekali yang diketahui secara umum tentang kejahatan siber. Seiring dengan perkembangan teknologi, kejahatan dunia digital juga ikut berkembang, yang mana terus mengembangkan jenis serangan, alat, dan teknik baru yang memungkinkan penyerang untuk menembus lingkungan yang lebih kompleks atau terkontrol dengan baik, dan menghasilkan kerusakan yang lebih besar dan bahkan tidak dapat dilacak (Andreea Bendovschi, 2015). Dilansir dari Identity Theft Resource Center (ITRC) Annual Data Breach Report pada tahun 2023, ditemukan 2.365 serangan siber yang mengakibatkan kebocoran data pada tahun 2023. Angka ini meningkat dari 1.584 pada tahun sebelumnya dan 754 pada tahun 2018. Penelitian yang dilakukan oleh IBM X-Force Threat Intelligence Index menambahkan, bahwa hampir setengah (43%) kasus dari kejahatan siber, merupakan ulah serangan malware, dimana 31% merupakan serangan *backdoor malware*, dengan diikuti 13% oleh ransomware. Belum lagi, Kaspersky Labs juga melaporkan bahwa sistem deteksi mereka menemukan bahwa adanya pertumbuhan malware yang signifikan sebesar 14% dari tahun 2023 sampai 2024.



Gambar 1. 1 Grafik Pertumbuhan Malware

(Dilansir dari : https://www.kaspersky.com)

Data ini secara jelas menimbulkan kewaspadaan yang mendalam terhadap keamanan data-data sensitif dalam informasi. Namun penerapan cyber security di beberapa negara masih sangat tertinggal, termasuk Indonesia. Melansir dari National Cyber Security Index (NCSI), skor keamanan siber di Indonesia hanyalah 63,64 dari 100 poin dan Indonesia berada di peringkat 49 dari 176 negara pada tahun 2023. Walaupun skor ini sudah meningkat lebih baik dari tahun 2022 dimana skor keamanan siber Indonesia hanya 38,92 dari 100 poin, skor pada tahun 2023 ini masih rendah dibanding negara-negara tetangga Indonesia seperti Singapura (71,33 dari 100 poin) dan Malaysia (79,22 dari 100 poin). Penelitian yang dilakukan oleh MIT Technology Review dalam The Cyber Defense Index tahun 2022/2023 mencatat bahwa keamanan siber Indonesia berada dalam posisi terendah pada urutan negara yang masuk dalam negara G-20.

Dengan keamanan siber yang kurang baik, Indonesia sering mengalami serangan siber yang merusak beberapa infrastruktur penting. Dilansir dari Badan Siber dan Sandi Negara (BSSN), tercatat bahwa ada 370,02 juta serangan siber terhadap Indonesia pada tahun 2022 dan sektor administrasi adalah sektor yang menjadi target utama serangan siber, dengan jumlah serangan 284,09 juta. Sebagai gambaran, kasus besar yang baru-baru ini terjadi pada tanggal 20 Juni 2024, dimana Pusat Data Nasional Sementara (PDNS) di Surabaya terserang oleh malware yang

teridentifikasi sebagai Brain Cipher, sebuah varian dari ransomware LockBit 3.0 (The Jakarta Post, 25 Juni 2024).

Dengan begitu, sekali lagi, keamanan siber yang memadai sangat diperlukan, terutama di Indonesia. Ancaman siber yang berbagai jenis dari fisik, logik, dan operasional, serta kesalahan manusia (human-error) menjadi ancaman serius pada saat ini. Proteksi data diidentifikasi sebagai strategi kunci dalam mengatasi ancaman cyber security (Novita et al. - Jurnal Ilmiah Sistem Informasi - 2023). Berdasarkan penelitian dari jurnal *Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking, American Journal of Computer Science and Technology,* oleh Ghelani et al. pada tahun 2022, salah satu langkah dalam proteksi data adalah dengan melakukan pendeteksian malware.

Penelitian yang dilakukan oleh Alsmadi & Alqudah dalam "A survey on heuristic malware detection techniques" - International Conference on Information Technology (ICIT) tahun 2021, menyebutkan bahwa ada 2 teknik dalam mendeteksi malware, teknik *static analysis* dan teknik *dynamic analysis*.

Teknik *static analysis* merupakan teknik yang mengumpulkan struktur kode program yang sedang diperiksa, dengan menggunakan beberapa alat seperti disassemble tool, decompile tool, debugger, atau source code analyzer, untuk memahami malware bekerja. Sementara itu teknik *dynamic analysis* mengedepankan proses menganalisis perilaku aplikasi dan analisis kode selama kode program dijalankan.

Alsmadi & Alqudah juga menyebutkan bahwa ada 3 metode dalam mendeteksi malware yaitu dengan menggunakan *signature-based, behaviour-based* dan *sandbox*. *Signature-based* mendeteksi malware dengan menggunakan pengambilan signature atau rangkaian bit untuk mengidentifikasi malware dan jenisnya, kemudian akan diupload ke dalam database cloud yang berisi data rangkaian bit atau signature yang sangat banyak dan luas. Setelah itu rangkaian bit yang malware yang diperiksa akan dicocokan dengan rangkaian bit yang ada dalam database. Jika rangkaian bit malware yang diperiksa cocok dengan rangkaian bit dalam database, maka basis data menandai bahwa file tersebut berbahaya, lalu rangkaian bit tersebut

akan ditolak oleh program anti-malware dari komputer dan dihapus. Metode *behaviour-based* lebih mengedepankan proses mendeteksi dan membedakan antara perilaku normal dan abnormal kode program untuk mengidentifikasi serangan malware yang diketahui dan tidak diketahui, lalu menemukan solusi yang sesuai. Aturan berbasis berat akan digunakan untuk menentukan seberapa besar risiko yang mungkin ditimbulkan oleh suatu kode program.

Menurut Alsmadi & Alqudah, salah satu kelemahan metode *signature-based* adalah metode ini hanya mampu mendeteksi malware yang sudah dikenal dan tercatat dalam database virus. Sehingga untuk mengatasi keterbatasan tersebut, diperlukan pendekatan *behaviour-based* dengan dikombinasikan dengan penggunaan pembelajaran mesin.

Penggunaan machine learning, seperti algoritma CNN dan LSTM, menjadi dapat menjadi langkah yang efektif dan efisien dalam mendeteksi dan mencegah serangan malware. Karena machine learning berbasis pada model yang dilatih secara terus-menerus, proses deteksi dan pencegahan dapat terus ditingkatkan dan dikembangkan, sehingga lebih efektif dalam menangkal malware canggih.

1.2 Perumusan Masalah

Rumusan masalah pada penelitian ini dapat dinyatakan sebagai berikut:

- Bagaimana cara mengimplementasikan algoritma Convolutional Neural Network (CNN) dan Long-Short Term Memory (LSTM) dalam mendeteksi malware berupa ransomware?
- Seberapa efektif penggunaan machine learning berbasis algoritma CNN dan LSTM dalam mendeteksi malware dibandingkan dengan sistem konvensional berbasis signature-based detection?

1.3 Batasan Masalah

Berdasarkan latar belakang dan rumusan masalah, batasan masalah dinyatakan sebagai berikut :

- Penelitian ini hanya akan membahas dan dibatasi pada pendeteksian jenis malware berupa ransomware. Malware lain seperti Trojan, adware, spyware, dan trojan tidak akan menjadi fokus penelitian ini .
- Penelitian juga dibatasi pada pendeteksian jenis file ".exe". File dengan jenis lain tidak akan menjadi fokus penelitian ini, tapi dapat menjadi bahan pertimbangan untuk penelitian selanjutnya.
- Penelitian hanya akan menggunakan behavior-based approach dengan dengan fokus analisis pada API calls. Pendekatan lain behavior-based atau pendekatan statis, tidak akan diimplementasikan, tetapi akan dibahas sebagai pembanding.
- Analisis dalam penelitian ini hanya akan menggunakan sandbox terisolasi CAPE v2. Sandbox-sandbox analisis lain tidak akan dibahas.
- Lingkup dataset: Dataset yang digunakan akan terbatas pada data perilaku ransomware yang relevan dan dapat diakses oleh peneliti.

1.4 Tujuan dan Manfaat

Berdasarkan latar belakang dan perumusan masalah, tujuan dan manfaat penelitian ini dinyatakan sebagai berikut :

- Mengembangkan aplikasi praktis berbasis web untuk menghasilkan sistem deteksi malware yang lebih adaptif, efisien, dan akurat dibandingkan sistem konvensional.
- Penelitian ini juga bertujuan untuk memberikan solusi untuk meningkatkan keamanan siber dan diharapkan dapat menjadi dasar bagi pengembangan alat pendeteksian malware berbasis AI untuk diterapkan di dunia nyata.
- Dalam bidang akademis, penelitian ini diharapkan mampu memberikan kontribusi dalam pengembangan ilmu pengetahuan khususnya pada penerapan machine learning dalam keamanan siber.

- Dalam bidang industri, penelitian ini diharapkan mampu menyediakan model pendeteksian ransomware berbasis AI yang dapat diterapkan secara nyata untuk meningkatkan keamanan sistem mereka.
- Dalam masyarakat, penelitian ini diharapkan membantu meningkatkan kesadaran tentang pentingnya keamanan siber dan memberikan solusi konkret dalam mencegah penyebaran malware.

1.5 Sistematika Penulisan

Sistematika penulisan dalam proposal penelitian ini disusun untuk memberikan panduan yang jelas dan sistematis dalam menjelaskan isi penelitian, mulai dari latar belakang hingga metode penelitian. Adapun sistematika penulisan dalam penelitian ini adalah sebagai berikut:

BAB I - PENDAHULUAN

Bab ini membahas dan menguraikan kerangka dasar yang menjadi landasan penelitian ini. Pembahasan meliputi penjabaran latar belakang masalah, rumusan masalah yang menjadi inti yang akan dijawab oleh penelitian ini, batasan-batasan masalah sebagai ruang lingkup penelitian, dan penjabaran tujuan spesifik sekaligus potensi manfaat penelitian baik secara teoritis maupun secara praktis.

BAB II - TINJAUAN PUSTAKA

Bab ini memuat dan menjabarkan landasan teoritis yang menjadi penopang penelitian ini. Pembahasan meliputi penjabaran konsep fundamental machine learning, pendefinisian malware dan juga ransomware, pendekatan deteksi berbasis perilaku (behavior-based) yang menjadi metode inti dari penelitian ini, penguraian arsitektur dan konsep model-model algoritma yang digunakan yaitu Convolutional Neural Network (CNN) dan Long Short-Term Memory (LSTM) dalam klasifikasi malware, dan yang terakhir penyajian ringkasan dari penelitian-penelitian sebelumnya guna memberikan konteks serta menunjukkan posisi dan kebaruan dari penelitian ini.

BAB III - METODOLOGI PENELITIAN

Bab ini memuat metodologi dan rencana, serta tahapan dalam penelitian ini. Bab ini berisi rancangan penelitian, tahapan penelitian, objek penelitian, model atau framework, serta teknik pengumpulan dan analisis data.

BAB IV - HASIL DAN PEMBAHASAN

Bab ini memuat dan membahas proses implementasi, pengujian dan juga hasil penelitian sesuai dengan rancangan dan metode penelitian yang sudah dibuat.

BAB V - KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran dari keseluruhan penelitian yang telah dilakukan.

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan temuan yang telah dipaparkan pada bab sebelumnya, dapat disimpulkan bahwa perancangan dan pembangunan, serta pengimplementasian aplikasi web deteksi ransomware menggunakan API call sequence telah berhasil dilakukan. Namun untuk menyimpulkan keefektifan dan untuk menjawab rumusan masalah kedua dari penelitian ini, perlu dilakukan perbandingan agar memberikan gambaran yang jelas tentang komparasi penelitian ini dengan penelitian sebelumnya.

Berdasarkan perbandingan dengan penelitian terdahulu, model deteksi ransomware yang dikembangkan dalam penelitian ini terbukti lebih unggul dan efektif. Dengan akurasi mencapai 99.51%, model ini menunjukkan performa yang signifikan karena beberapa alasan utama:

1) Pendekatan Unggul: Tidak seperti analisis statis (Hadiprakoso et al., 2021; akurasi 96.94%), pendekatan analisis dinamis yang digunakan telah divalidasi menggunakan dataset yang sepenuhnya diambil berbeda dengan data latih, membuktikan efektivitasnya dalam skenario dunia nyata.
2) Konteks Krusial Terjaga: Berbeda dengan metode yang mengubah API calls menjadi signature terstruktur (Savenko et al., 2020; akurasi 96.56%), model Bidirectional LSTM yang dikembangkan berhasil mempertahankan informasi kontekstual dan urutan API calls yang krusial.
3) Generalisasi Terbukti: Meskipun ada penelitian dengan akurasi lebih tinggi (Satrya Bhayangkara et al., 2023; 99.99%), hasil tersebut didasarkan pada dataset yang sangat kecil. Sebaliknya, model dalam penelitian ini divalidasi pada set data uji yang besar dan diambil berbeda dengan data latih, membuktikan kemampuan generalisasi yang kuat dan andal.

Dengan demikian, dapat disimpulkan bahwa analisis dinamis berbasis perilaku API calls menggunakan model deep learning merupakan solusi yang lebih efektif dan dapat diandalkan untuk mendeteksi ancaman ransomware.

5.2 Saran

Berdasarkan hasil penelitian ini, terdapat beberapa peluang pengembangan lebih lanjut yang dapat dilakukan di masa depan. Saran utama untuk penelitian selanjutnya adalah pengembangan model menjadi arsitektur model multi-input hibrida CNN-LSTM yang lebih canggih. Model ini akan memproses dua jenis data secara bersamaan, yaitu menggunakan CNN untuk menganalisis sekuens n-gram untuk mengidentifikasi pola-pola lokal yang signifikan, dan yang kedua menggunakan LSTM untuk memahami konteks temporal dari sekuens API calls utuh.

Output dari CNN dan LSTM tersebut kemudian digabungkan untuk menghasilkan prediksi akhir. Dengan memanfaatkan kemampuan CNN dalam mengenali motif/pola perilaku dan LSTM dalam memahami alur/temporal eksekusi secara keseluruhan, pendekatan ini diharapkan dapat meningkatkan akurasi dan performa deteksi terhadap taktik-taktik ransomware yang kompleks.

DAFTAR PUSTAKA

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press. http://www.deeplearningbook.org

Aalam, Z., Kumar, V., & Gour, S. (2021). A review paper on hypervisor and virtual machine security. *Journal of Physics: Conference Series*, *1950*(1), 012027. https://doi.org/10.1088/1742-6596/1950/1/012027

Alsmadi, T., & Alqudah, N. (2021). A Survey on malware detection techniques. *2021 International Conference on Information Technology (ICIT)*, 371–376. https://doi.org/10.1109/icit52682.2021.9491765

Bajpai, P., & Enbody, R. (2020, July). An empirical study of API calls in ransomware. *2020 IEEE International Conference on Electro Information Technology (EIT)*. https://doi.org/10.1109/eit48999.2020.9208284

Bhavesh M. Patel, B. M., & Sule, M. (2023). TOKENIZATION TECHNIQUES IN NLP:A COMPREHENSIVE REVIEW. *International Journal Of Advance Research And Innovative Ideas In Education*, *9*(1–2023). https://doi.org/16.0415/IJARIIE-22082

Botwright, R. (2023). *Malware analysis: Digital forensics, cybersecurity, and incident response*. Rob Botwright.

Catak, F. O. (2020, August 25). Deep Learning and LSTM based Malware Classification. *TDS Archive*. https://medium.com/data-science/deep-lstm-based-malware-analysis-6b36ac247f34

Cybellium. (2024). *Study guide to malware analysis: A comprehensive guide to learn malware analysis*. Cybellium Ltd.

Elyas, M. I. N. (2019). *Penggunaan Metode Behavior Based Detection Untuk Deteksi Ransomware Dengan Cara Mengawasi Perilaku Aplikasi Pada Data* (p. 33) [Thesis, Universitas Islam Indonesia]. http://hdl.handle.net/123456789/16081

GeeksforGeeks. (2021, May 30). NGram language modelling with NLTK. *GeeksforGeeks*. https://www.geeksforgeeks.org/n-gram-language-modelling-with-nltk/

Hadiprakoso, R. B., Aditya, W. R., & Pramitha, F. N. (2022). ANALISIS STATIS

DETEKSI MALWARE ANDROID MENGGUNAKAN ALGORITMA SUPERVISED MACHINE LEARNING. *Cyber Security Dan Forensik Digital*, *5*(1), 1–5. https://doi.org/10.14421/csecurity.2022.5.1.3116

Hadiprakoso, R. B., Qomariasih, N., & Yasa, R. N. (2021). IDENTIFIKASI MALWARE ANDROID MENGGUNAKAN PENDEKATAN ANALISIS HIBRID DENGAN DEEP LEARNING. *Jurnal Teknologi Informasi Universitas Lambung Mangkurat (JTIULM)*, *6*(2), 77–84. https://doi.org/10.20527/jtiulm.v6i2.82

Hartono, B. (2023). Ransomware: Memahami ancaman Keamanan Digital. *Bincang Sains Dan Teknologi*, *2*(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

Iqbal, S., Ullah, A., Adlan, S., & Soobhany, A. R. (2022). Malware prediction using LSTM networks. In *Lecture Notes in Networks and Systems* (pp. 583–604). Springer Nature Singapore. https://doi.org/10.1007/978-981-16-7618-5_51

Khalda, K., & Wibowo, D. K. (2025). Malware behavior analysis using static and dynamic analysis approaches. *Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi*, *4*(1), 1–8. https://doi.org/10.20885/snati.v4.i1.1

Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016). Deep learning for classification of malware system call sequences. In *Lecture Notes in Computer Science* (pp. 137–149). Springer International Publishing. https://doi.org/10.1007/978-3-319-50127-7_11

Kothamali, P. R., & Banik, S. (2022, March 14). *Limitations of signature-based threat detection*. Unknown. https://www.researchgate.net/publication/388494583_Limitations_of_Signature-Based_Threat_Detection

Okut, H. (2021). Deep learning for subtyping and prediction of diseases: Long-Short term memory. In *Deep Learning Applications*. IntechOpen. https://doi.org/10.5772/intechopen.96180

QEMU. (n.d.). Retrieved June 14, 2025, from https://www.qemu.org/

R, R. R., S, N., R, S., & S, T. (2024). Malware analysis using Sandbox. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4708146

Satrya Bhayangkara, D., Dwi Putranto, H., Toriq, F., & Wijayanto, F. (2023). Analisis Static Malware Menggunakan Algoritma Random Forest Machine Learning. *Jurnal Teknologi Informasi*, *9*(2).

Savenko, O., Nicheporuk, A., Hurman, I., & Lysenko, S. (2020). Dynamic Signature-based Malware Detection Technique Based on API Call Tracing. *CEUR Workshop Proceeding*, *2393*(278).

Wang, S., Li, Z., & Zhao, X. (2022). The application of convolutional neural network in malware images classification. *Advances in Social Science, Education and Humanities Research*. https://doi.org/10.2991/assehr.k.220110.047

What is CAPE? — CAPE Sandbox v2.2 Book. (n.d.). Retrieved June 10, 2025, from https://capev2.readthedocs.io/en/latest/introduction/what.html

Yakub, H., Daniawan, B., Wijaya, A., & Damayanti, L. (2024). Sistem informasi e-commerce berbasis website Dengan Metode pengujian user acceptance testing. *JSITIK: Jurnal Sistem Informasi Dan Teknologi Informasi Komputer*, *2*(2), 113–127. https://doi.org/10.53624/jsitik.v2i2.362

(2022). *Jurnal Teknologi Informasi*, *8*(2). https://doi.org/10.52643/jti.v8i2

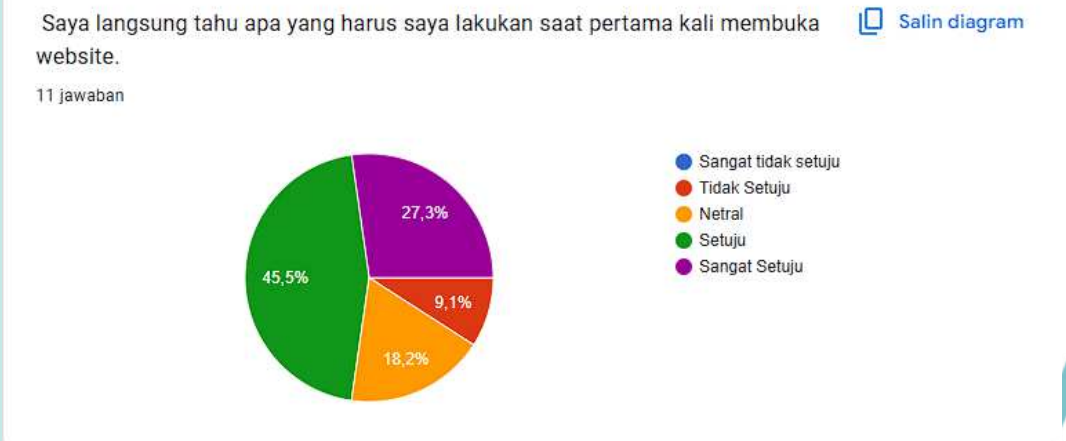
DAFTAR RIWAYAT HIDUP

Benaya Adi Sahat Dwiyanto

Lahir di Depok, 11 Desember 2002. Anak kedua dari 2 bersaudara kembar. Lulus dari SD Mardi Yuana, Depok pada tahun 2015, SMPN 5 Depok pada tahun 2018, dan SMAN 11 Depok pada tahun 2021. Saat ini menempuh Pendidikan Sarjana Terapan pada Program Studi Teknik Informatika di Politeknik Negeri Jakarta. Tertarik pada bidang Data Science dan Quantitatif.

LAMPIRAN

Lampiran 1 Pie Chart Kuesioner UAT Uji Coba Aplikasi Web Sysmal

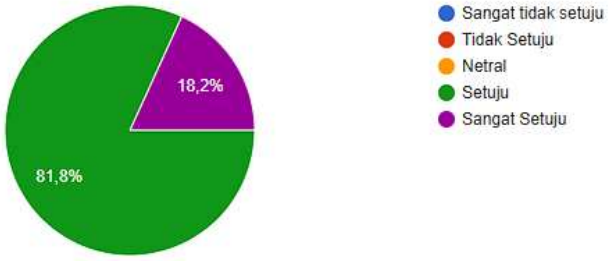


(Lanjutan)

Proses untuk mengunggah file tidak membingungkan sama sekali.

Salin diagram

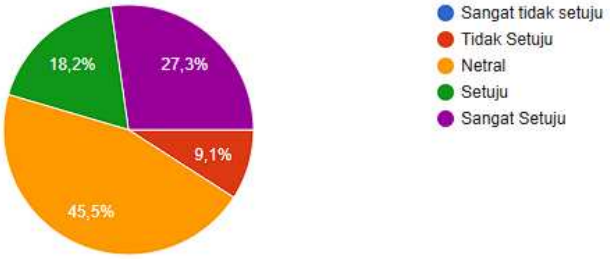
11 jawaban



Hasil deteksi (misalnya, tulisan "Malware" atau "Benign") sangat jelas dan langsung ke intinya.

Salin diagram

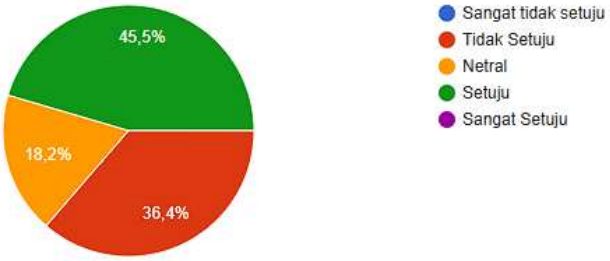
11 jawaban



Saya tidak memerlukan penjelasan tambahan untuk mengerti arti dari hasil yang ditampilkan.

Salin diagram

11 jawaban

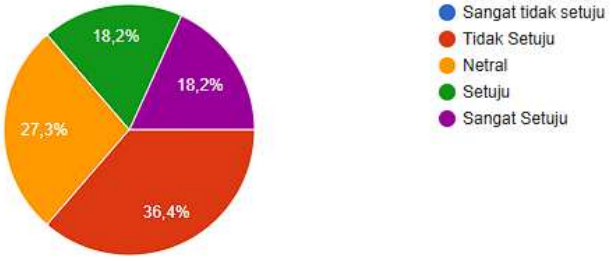


(Lanjutan)

Waktu tunggu dari selesai unggah hingga hasil muncul terasa cepat dan wajar.

Salin diagram

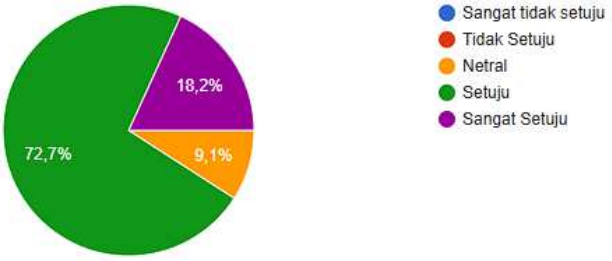
11 jawaban



Desain yang sederhana dan fokus membuat website ini terasa profesional.

Salin diagram

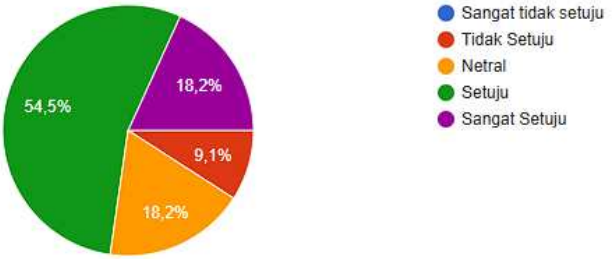
11 jawaban



Meskipun hasilnya tunggal (bukan dari banyak sumber seperti VirusTotal), saya merasa cukup percaya pada kesimpulannya untuk pengecekan awal.

Salin diagram

11 jawaban



(Lanjutan)

Menurut saya, aplikasi ini sudah cukup untuk kebutuhan melakukan pengecekan file secara cepat.

Salin diagram

11 jawaban