DETEKSI *EXPLOIT REVERSE* HTTPS MENGGUNAKAN METODE *RANDOM FOREST*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer (S1)

OLEH:

ALESSANDRO LUMBAN TUNGKUP

09011382025143

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI EXPLOIT REVERSE HTTPS MENGGUNAKAN METODE RANDOM FOREST

Sebagai salah satu syarat untuk penyelesaian studi di
Program Studi S1 Sistem Komputer

Oleh:

ALESSANDRO LUMBAN TUNGKUP

09011382025143

Pembimbing 1 : **Prof. Deris Stiawan, M.T., Ph.D.**

NIP. 197806172006041002

Pembimbing 2 : **Nurul Afifah, M.Kom.**

NIP. 199211102023212049

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T

196612032006041001

AUTHENTICATION PAGE

FINAL TASK

DETECTION OF REVERSE HTTPS EXPLOIT USING THE RANDOM FOREST METHOD

Submitted To Complete One Of The Requirements For Obtaining A Bachelor's Degree in Computer Science

By:

ALESSANDRO LUMBAN TUNGKUP

09011382025143

Supervisor	**: Prof. Deris Stiawan, M.T., Ph.D.**
	NIP. 197806172006041002
Co-Supervisor	**: Nurul Afifah, M.Kom.**
	NIP. 199211102023212049

Head Of The Computer System Departement

Dr. Ir. Sukemi, M.T

196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 09 Mei 2025

Tim Penguji :

1. **Ketua : Dr. Ahmad Zarkasi, M.T.**
2. **Penguji : Dr. Ahmad Heryanto, S.Kom, M.T.**
3. **Pembimbing I : Prof. Ir. Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing II : Nurul Afifah, M.Kom.**

Mengetahui.
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Alessandro Lumban Tungkup

NIM : 09011382025143

Judul : Deteksi *Exploit Reverse* HTTPS Menggunakan Metode *Random Forest*

Hasil Pengecekan Software *iThenticate/Turnitin* : 6%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil pengjiplakan 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 dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, 13 Juni 2025

Yang menyatakan

Alessandro Lumban Tungkup

NIM. 09011382025143

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan atas hadirat Tuhan Yang Maha Esa karena dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan tugas akhir dengan judul **"Deteksi *Exploit Reverse* HTTPS Menggunakan Metode *Random Forest*"**.

Pada penyusunan tugas akhir ini tidak terlepas dari peran berbagai pihak yang telah memberikan dukungan doa, semangat, motivasi dan bimbingan pada penulis. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Tuhan Yang Maha Esa. yang telah memberikan Kesehatan dan Kesempatan kepada penulis dalam penyusunan tugas akhir ini.
2. Kedua orang tua tercinta yang selalu memberikan dukungan moral maupun finansial, serta do'a yang tiada hentinya.
3. Adik-adik saya (Melisa Sandrina, Bintang Marcello, dan Keisha Rebeka) yang selalu memberikan semangat dan do'a.
4. Bapak Prof. Dr. Erwin, M.Si selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Abdurahman, S.Kom., M.Han. selaku Dosen Pembimbing Akademik.
7. Bapak Deris Stiawan, M.T., Ph.D., IPU., ASEAN-Eng., CPENT selaku Pembimbing Utama Tugas Akhir Penulis yang telah meluangkan waktu untuk membimbing dan memberikan motivasi selama pengerjaan Tugas Akhir.
8. Mbak Nurul Afifah, M.Kom. selaku Pembimbing Pendamping Tugas Akhir yang telah meluangkan waktu untuk membimbing penulis dalam pengerjaan Tugas Akhir dari awal sampai dengan penulisan laporan Tugas Akhir.

9. Mba Sari Anhar selaku admin yang telah membantu dalam proses administrasi Tugas Akhir Penulis.
10. Teman-teman satu kelompok riset yang selalu memberikan semangat dan solusi kepada penulis yaitu Muhammad Bayu Cailendra, Azzan Daffa Al Kautsar, dan Rafi Fajar Tsani .
11. Teman-teman kelas saya yang selalu memberi support yaitu Salman Husein, Dede Rizky Kurniawan, M. Arko Patikawa dan teman-teman lainnya.
12. Teman-teman seperjuangan Jurusan Sistem Komputer Unggulan 2020.
13. Teman-teman terdekat saya yang selalu memberi support yaitu Anzu, Holy, Agustinus, Bram, Jeims Yosua, Sengon dan Bara.
14. Seluruh pihak yang tidak dapat penulis sebutkan satu per satu, yang telah memberikan semangat serta doa.
15. Almamater

Penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis dengan senang hati menerima kritik dan saran serta masukkan dari pembaca yang bersifat membangun agar lebih baik lagi dikemudian hari. Penulis berharap semoga laporan ini dapat bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya. Demikian yang dapat penulis sampaikan.

Palembang, Juni 2025

Penulis,

Alessandro Lumban Tungkup

NIM. 09011382025143

DETEKSI EXPLOIT REVERSE HTTPS MENGGUNAKAN METODE RANDOM FOREST

Alessandro Lumban Tungkup (09011382025143)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email: 09011382025143@student.unsri.ac.id

ABSTRAK

Exploit Reverse HTTPS adalah salah satu teknik serangan malware yang dimanfaatkan oleh pelaku untuk mengeksploitasi celah keamanan pada lapisan HTTPS suatu aplikasi atau sistem, dengan tujuan mencuri data penting dari target. Dalam penelitian ini, digunakan dataset mentah berformat .pcap yang berasal dari COMNETS *Research Lab* Universitas Sriwijaya. Dataset tersebut dikumpulkan melalui skenario eksperimen yang dirancang secara realistis untuk mendeteksi kerentanan pada protokol HTTPS menggunakan pendekatan *Dynamic Analysis* serta algoritma *Random Forest*. Hasil analisis menunjukkan bahwa algoritma *Random Forest* memiliki kemampuan yang tinggi dalam mengidentifikasi serangan *Reverse* HTTPS, dengan akurasi deteksi mencapai 96,58%.

Kata Kunci : *Android, Malware, Reverse HTTPS, Dynamic Analysis, Random Forest.*

DETECTION OF REVERSE HTTPS EXPLOIT USING THE RANDOM FOREST METHOD

Alessandro Lumban Tungkup (09011382025143)

Department Of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email : 09011382025143@student.unsri.ac.id

ABSTRACT

Reverse HTTPS Exploit is a type of malware attack technique used by attackers to exploit vulnerabilities in the HTTPS layer of an application or system, aiming to steal sensitive data from the target. This study utilized raw dataset files in .pcap format provided by the COMNETS Research Lab at Sriwijaya University. The data was collected through realistically designed experimental scenarios to detect vulnerabilities in the HTTPS protocol using Dynamic Analysis and the Random Forest algorithm. The results demonstrate that the Random Forest method is highly effective in identifying Reverse HTTPS attacks, achieving a detection accuracy of 96.58%.

Keywords : Android, Malware, Reverse HTTPS, Dynamic Analysis, Random Forest

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin berkembang, perangkat *android* telah menjadi sasaran utama berbagai ancaman keamanan, khususnya *malware*. *Malware* pada android dapat menyusup melalui aplikasi berbahaya, situs *web* yang tidak aman, atau eksploitasi celah keamanan sistem. Seiring dengan meningkatnya pengguna *android* dalam kehidupan sehari-hari, serangan *malware* juga semakin canggih, sehingga menuntut langkah-langkah keamanan yang lebih efektif untuk melindungi pengguna dari potensi risiko yang merugikan.

Eksploitasi *Reverse* HTTPS adalah teknik serangan dimana malware dalam sistem korban membuat koneksi luar ke *server* penyerang melalui HTTPS, memungkinkan kontrol jarak jauh tanpa terdeteksi oleh *firewall* atau NAT. Teknik ini sering digunakan dalam *Remote Accsess Trojan* atau *Metasploit payloads*, karena lalu lintas HTTPS yang terenkripsi menyerupai komunikasi *web* normal, sehingga sulit dideteksi oleh sistem keamanan.

Program dengan tujuan yang tidak baik dan tentu saja merugikan perangkat korban yaitu *Malware,* bisa melakukan eksploitasi seperti pencurian data, menghambil alih perangkat atau hal merugikan lainnya pada data atau perangkat korban [1]. Dengan pertumbuhan teknologi yang cepat, malware menjadi salah satu aspek keamanan yang paling signifikan [2]. Kategori utama di mana malware dapat dikelompokkan meliputi virus, *worm*, *Trojan*, *ransomware*, *rootkit, botnet*, dan lain-lain [3] [4]. Terdapat berbagai definisi untuk *malware* yang diberikan oleh banyak peneliti tergantung pada dampak merugikan yang dihasilkannya. Penelitian ini akan mempelajari dataset berisi *malware* dan melakukan deteksi apakah benar terdapat serangan *malware* didalamnya [5].

Perilaku *malware* dipelajari dalam konteks serangan terhadap perangkat mobile membutuhkan dataset yang digunakan merupakan hasil penelitian pada

kasus *cyber attack* khususnya pada lingkungan perangkat *mobile* yaitu dataset *Victim Reverse* HTTPS, dataset ini mengusulkan lalu lintas jaringan yang dibuat dengan skenario percobaan mendekati kejadian nyata untuk meneliti aktivitas komunikasi trojan APK yang dibuat *dengan tools open source Metasploit* pada perangkat Android [5]. Adapun jenis eksploitasi yang digunakan adalah *reverse* TCP dan *reverse* HTTPS yang disematkan pada sebuah APK normal/jinak dan bisa digunakan oleh korban [6]. Dataset yang digunakan dalam penelitian ini memiliki kondisi data yang tidak seimbang atau *imbalanced* akan mempengaruhi hasil kinerjanya. Untuk mengatasi data yang tidak seimbang tersebut maka akan dilakukan teknik resampling dengan oversampling menggunakan *Random Oversampling*.

Penelitan ini sendiri akan berfokus pada serangan eksploitasi berupa *reverse* HTTPS yang terdapat pada dataset. *Hypertext Transfer Protocol Secure* (HTTPS) memiliki pengertian yang sama dengan HTTP yaitu protokol meminta atau menjawab antara *client* dan server. Sebuh *client* HTTP seperti *web browser*, biasanya memulai permintaan dengan membuat hubungan TCP/IP ke port tertentu, hanya saja https memiliki kelebihan fungsi di bidang keamanan (*secure*). Dengan menggunakan *Secure Socket Layer* (SSL) atau *Transport Layer Security* (TLS) sebagai *sublayer* di bawah http aplikasi *layer* yang biasa. Teknologi https protokol mencegah kemungkinan "dicurinya" informasi penting yang dikirimkan selama proses komunikasi berlangsung antara *user* dengan *web server* atau sebaliknya [7]. HTTPS bukan protokol yang terpisah, tetapi mengacu pada kombinasi dari interaksi HTTP normal melalui *Socket Layer* terenkripsi SSL (Secure) atau *Transport Layer Security* (TLS) mekanisme transportasi. Hal ini menjamin perlindungan yang wajar dari penyadapan dan serangan [8].

Penelitian ini akan menggunakan *Machine Learning* sebagai metode untuk mendeteksi dataset nya. *Machine Learning* adalah cabang dari kecerdasan buatan yang berfokus pada pengembangan aplikasi dengan belajar dari data tanpa secara eksplisit memprogram cara tugas yang dipelajari dilakukan. Metode *Machine Learning* tradisional membuat prediksi berdasarkan data yang telah diambil dari hasil penelitian terkait yang telah

dilakukan sebelumnya. Siklus hidup proses *machine learning* terdiri dari beberapa langkah berurutan. Mereka adalah ekstraksi data, pra-pemrosesan data, pemilihan fitur, pelatihan model, evaluasi model, dan implementasi model [3].

Model machine learning yang akan digunakan adalah *Random Forest*. *Random Forest* merupakan salah satu metodologi *machine learning* yang efektif untuk klasifikasi dan regresi, dan juga dapat digunakan untuk segmentasi gambar ketika data pelatihan terbatas. Pengklasifikasi *random forest* telah berhasil digunakan untuk berbagai tujuan seperti segmentasi seperti melakukan validasi adanya serangan malware yang ada terekam pada suatu dataset dan pendekatan ini dapat digunakan untuk mendeteksi serangan malware yang ada pada dataset [9]. Konsep dari *Random Forest* ini akan menghasilkan "hutan" dengan gabungan dari sejumlah *Decision Tree*. *Random Forest* dalam proses pengklasifikasi akan dibagi menjadi kelas prediksi dan kelas dengan suara yang terbanyak akan menjadi model prediksi [10]. Proses klasifikasi yang dilakukan akan bermanfaat pada keamanan c*yber* untuk menganalisa file aplikasi *exploit reverse* HTTPS yang terindikasi *malware* atau tidak, sehingga dapat membantu mengatasi ancaman yang datang dari file APK.

Penelitian yang berjudul *AI-HydRa: Advanced hybrid approach using random forest and deep learning for malware classification* [11], MLP dynamic mencapai akurasi tertinggi sebesar 96.1% dengan 205 node. Meskipun performa MLP static lebih rendah, model ini stabil dengan 20–38 node dan tetap penting dalam sistem klasifikasi hibrida. Penelitian ini bertujuan mengembangkan model deteksi malware berbasis *machine learning* hibrida yang lebih akurat dalam mencegah penyebaran *malware*, termasuk serangan adversarial dan zero-day. Dengan menggabungkan fitur statis dan dinamis serta aturan voting, model ini meningkatkan deteksi hingga 19% dan dapat mengidentifikasi *malware* dalam 60,9 detik tanpa analisis manual.

Penelitian yang berjudul *Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset* [12],

memperkenalkan *UGRansome2024*, dataset baru untuk deteksi *ransomware* yang dioptimalkan dengan teknik rekayasa fitur intuitif. Menggunakan *Random Forest*, dataset ini mencapai akurasi klasifikasi 96% dalam mengidentifikasi ransomware yang tidak biasa. Temuan menunjukkan varian *ransomware* seperti EDA dan Globe memiliki dampak finansial terbesar. Penelitian ini menyoroti pentingnya pembelajaran mesin dalam deteksi *ransomware* dan mendorong pengembangan dataset lebih lanjut serta metode deteksi baru.

Penelitian yang berjudul *Ransomware Detection Using Aggregated Random Forest Technique with Recent Variants* [13], Model yang diusulkan memanfaatkan Random Forest dalam pipeline end-to-end, menunjukkan akurasi 94,2% dalam perbandingan dengan tiga model canggih lainnya. Penelitian ini bertujuan mengembangkan sistem deteksi *malware* yang efektif dengan menggabungkan metode deteksi berbasis perilaku dan tanda tangan menggunakan teknik pembelajaran mesin (ML) dan *deep learning*. Fokusnya adalah menjelaskan tantangan dalam deteksi *malware*, mengklasifikasikan teknik ML yang digunakan, dan mengevaluasi pendekatan pembelajaran mendalam.

Penelitian yang berjudul *Ransomware Detection using Random Forest Technique* [14], menggunakan model *random forest* dan mendapatkan akurasi sebesar 97.74%. Penelitian ini berujuan untuk mengembangkan teknik deteksi ransomware menggunakan *machine learning*, khususnya algoritma *random forest*. *Ransomware* merupakan jenis malware yang mengenkripsi file pengguna dan meminta tebusan untuk kunci dekripsi. Dengan memanfaatkan fitur dari byte mentah *file*, penelitian ini menguji berbagai parameter *random forest* untuk menghasilkan model yang efektif dan akurat dalam mendeteksi ransomware.

Penelitian yang berjudul *Zero-Day Ransomware Detection via Assembly Language Bytecode Analysis and Random Forest Classification* [15], mendapatkan hasil 93,5%. Penelitian ini bertujuan untuk analisis mengenai pentingnya fitur dalam model ini memberikan wawasan lebih dalam mengenai

perilaku *ransomware* secara mendetail, serta mengidentifikasi *bytecode* mana yang paling terkait dengan aktivitas *ransomware*.

Berdasarkan pembahasan di atas, penulis akan melakukan deteksi eksploitasi *reverse* HTTPS dari aplikasi dalam *network traffic* menggunakan metode *random forest*. Judul dari tugas akhir ini adalah "Deteksi *Exploit Reverse* HTTPS dari Aplikasi di *Network Traffic* dengan Metode *Random Forest*". Diharapkan penelitian ini dapat memberikan hasil yang baik dan menjadi referensi bagi penelitian terkait.

1.2 Rumusan Masalah

Rumusan masalah penelitian Tugas Akhir ini adalah:

1. Bagaimana cara mengekstraksi fitur dapat diterapkan pada dataset *Victim Reverse* HTTPS?
2. Bagaimana cara menerapkan *Dynamic Analysis* dalam mendeteksi *Behavior Exploit Reverse* HTTPS pada dataset *Victim Reverse* HTTPS?
3. Bagaimana menvalidasi hasil dari deteksi menggunakan metode *Random Forest* dan tingkat keakuratan model dalam mendeteksi pada dataset?

1.3 Batasan Masalah

Agar penelitian mengarah sesuai tujuan yang diharapkan, maka diperlukannya batasan masalah dalam penelitian ini. Adapun batasan masalah tersebut adalah sebagai berikut:

1. Penelitian ini menggunakan dataset *Mobile-TrojanMetasploit Traffic*, yaitu skenario 2 *Victim Reverse* HTTPS.
2. Penelitian ini akan berfokus pada penerapan *Dynamic Analysis* dan algoritma *Random Forest* untuk mendeteksi serangan pada dataset *Victim Reverse* HTTPS.
3. *Random Oversampling* digunakan untuk menangani masalah ketidakseimbangan kelas pada dataset *Victim Reverse* HTTPS.
4. Metode evaluasi performa yang digunakan mencakup akurasi, recall, presisi dan skor F1.

1.4 Tujuan Penelitian

Tujuan dari penelitian Tugas Akhir ini antara berikut:

1. Mengekstraksi dataset dari format .pcap menjadi format .csv menggunakan *tools CICFlowMeter.*
2. Menerapkan algoritma *Random Forest* untuk melakukan deteksi *Exploit Reverse HTTPS*.
3. Mengevaluasi performa deteksi yang diperoleh melalui analisis dinamis dan algoritma *Random Forest* guna menentukan model paling optimal.

1.5 Manfaat Penelitian

Manfaat penelitian dari tugas akhir ini antara lain:

1. Meningkatkan pemahaman terkait pemrosesan dataset menggunakan CIC*FlowMeter*.
2. Memahami *Behavior Exploit Reverse* HTTPS menggunakan analisis dinamis dan algoritma *Random Forest.*
3. Meningkatkan kemampuan analisis dan pemecahan masalah dalam bidang keamanan siber.

1.6 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penelitian ini mencakup beberapa tahapan berikut:

1.6.1 Studi Pustaka (Literature)

Pada tahap ini, referensi yang berhubungan dengan perilaku *Exploit Reverse HTTPS,* analisis dinamis*,* algoritma *Random Forest*, dan aspek lain yang mendukung penelitian dikumpulkan sebagai bahan kajian.

1.6.2 Pengumpulan Data

Tahapan ini merupakan langkah awal dalam proses penelitian, dimana pengumpulan data dilakukan melalui beberapa metode berikut:

a. Analisis Dinamis

Langkah ini bertujuan untuk mengidentifikasi karakteristik serangan atau aktivitas serangan atau aktivitas mencurigakan dalam dataset *Victim Reverse* HTTPS.

b. Identifikasi Sumber Data

Identifikasi sumber data dilakukan proses penentuan jenis, asal dan karakteristik data untuk memastikan bahwa analisis yang dilakukan berkaitan dan berhubungan dengan dataset yang akan diteliti.

c. Ekstraksi Data

Ekstraksi data dilakukan terhadap sumber data yang telah diidentifikasi. Dalam penelitian ini, ekstraksi diterapkan pada dataset untuk kemudian dianalisis lebih lanjut.

1.6.3 Processing

Pada tahap ini, data yang telah diekstraksi akan diperiksa melalui langkah-langkah berikut:

a. Pembuatan Label

Proses ini bertujuan untuk memberikan label pada dataset guna mengklasifikasikannya kedalam kategori *Benign* atau *Reverse* HTTPS.

b. Analisis Data Eksploratif

Analisis data eksploratif (*Exploratory Data Analysis*) merupakan langkah awal dalam menganalisis data untuk memahami struktur, pola, anomali dan kualitasnya.

1.6.4 Analisis

Analisis dilakukan dengan membangun model *Random Forest* berdasarkan dataset *Victim Reverse* HTTPS. Evaluasi terhadap performa model dilakukan dengan menggunakan metrik seperti akurasi, presisi, *recall*, dan skor F1.

1.6.5 Kesimpulan dan Saran

Setelah analisis selesai, hasil penelitian dirangkum dan diberikan rekomendasi untuk penelitian selanjutnya. Selain itu, dokumentasi hasil penelitian serta interpretasi kesimpulan yang diperoleh juga disajikan.

1.7 Sistematika Penulisan

Struktur sistematika yang digunakan dalam penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, serta sistematika yang digunakan dalam penelitian ini.

BAB II TINJAUAN PUSTAKA

Bab ini menguraikan konsep-konsep terkait yang penting seperti *Reverse* HTTPS, analisis dinamis, algoritma *Random Forest* dan dataset yang digunakan. Selain itu, juga disajikan kajian terkait penerapan dari analisis dinamis malware dan *Random Forest*.

BAB III METODOLOGI PENELITIAN

Bab ini membahas metode yang diterapkan dalam penelitian, mulai dari diagram alur hingga tahapan perancangan sistem yang digunakan dalam penelitian ini.

BAB IV HASIL DAN ANALISIS

Bab ini menjelaskan hasil pengolahan data yang telah dikumpulkan, kemudian dilakukan analisis untuk memperoleh informasi yang relevan dan akurat.

BAB V KESIMPULAN DAN SARAN

Bab ini menyajikan kesimpulan dari penelitian serta memberikan rekomendasi untuk pengembangan lebih lanjut di masa mendatang.

DAFTAR PUSTAKA

[1] D. Gupta and R. Rani, "Improving malware detection using big data and ensemble learning," *Comput. Electr. Eng.*, vol. 86, p. 106729, 2020, doi: 10.1016/j.compeleceng.2020.106729.

[2] R. Kumar, "Zero-Day Malware Detection and Effective Malware Analysis," 2022.

[3] A. Qamar, A. Karim, and V. Chang, "Mobile malware attacks: Review, taxonomy & future directions," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 887–909, 2019, doi: 10.1016/j.future.2019.03.007.

[4] A. S. Shamili, C. Bauckhage, and T. Alpcan, "Malware detection on mobile devices using distributed machine learning," *Proc. - Int. Conf. Pattern Recognit.*, pp. 4348–4351, 2010, doi: 10.1109/ICPR.2010.1057.

[5] A. S. Review, "Android Mobile Malware Detection Using Machine Learning :," pp. 1–34, 2021.

[6] "Mobile-TrojanMetasploit Traffic Dataset Sebagai bentuk upaya untuk melakukan penelitian pada kasus," pp. 2–5.

[7] A. A. Zabar and F. Novianto, "Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux," *Komputa J. Ilm. Komput. dan Inform.*, vol. 4, no. 2, pp. 69–74, 2015, doi: 10.34010/komputa.v4i2.2427.

[8] N. A. Azeez, O. E. Odufuwa, S. Misra, J. Oluranti, and R. Damaševičius, "Windows PE malware detection using ensemble learning," *Informatics*, vol. 8, no. 1, 2021, doi: 10.3390/informatics8010010.

[9] I. A. Khan, H. Birkhofer, D. Kunz, D. Lukas, and V. Ploshikhin, "A Random Forest Classifier for Anomaly Detection in Laser-Powder Bed Fusion Using Optical Monitoring," *Materials (Basel).*, vol. 16, no. 19, pp. 1–19, 2023, doi: 10.3390/ma16196470.

[10] G. Ngo, R. Beard, and R. Chandra, "Evolutionary bagging for ensemble learning," *Neurocomputing*, vol. 510, pp. 1–14, 2022, doi: 10.1016/j.neucom.2022.08.055.

[11] S. Yoo, S. Kim, S. Kim, and B. B. Kang, "AI-HydRa: Advanced hybrid approach using random forest and deep learning for malware

classification," *Inf. Sci. (Ny).*, vol. 546, pp. 420–435, 2021, doi: 10.1016/j.ins.2020.08.082.

[12] P. Azugo, H. Venter, and M. Wa Nkongolo, "Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset," 2021.

[13] J. Rafapa and A. Konokix, "Technique with Recent Variants Ransomware Detection Using Aggregated Random Forest Technique with Recent Variants," 2024.

[14] B. M. Khammas, "Ransomware Detection using Random Forest Technique," *ICT Express*, vol. 6, no. 4, pp. 325–331, 2020, doi: 10.1016/j.icte.2020.11.001.

[15] E. Fevid, C. Walsh, L. Russo, E. Fevid, C. Walsh, and L. Russo, "Zero-Day Ransomware Detection via Assembly Language Bytecode Analysis and Random Forest Classification," 2024.

[16] S. A. Roseline, S. Geetha, S. Kadry, and Y. Nam, "Intelligent Vision-Based Malware Detection and Classification Using Deep Random Forest Paradigm," *IEEE Access*, vol. 8, pp. 206303–206324, 2020, doi: 10.1109/ACCESS.2020.3036491.

[17] A. Kumar, K. Abhishek, S. K. Shandilya, and M. R. Ghalib, "Malware analysis through random forest approach," *J. Web Eng.*, vol. 19, no. 5–6, pp. 795–818, 2020, doi: 10.13052/jwe1540-9589.195610.

[18] S. D. Alotaibi *et al.*, "Bioinspired artificial intelligence based android malware detection and classification for cybersecurity applications," *Alexandria Eng. J.*, vol. 100, no. April, pp. 142–152, 2024, doi: 10.1016/j.aej.2024.05.038.

[19] N. Gregório, J. Bispo, J. P. Fernandes, and S. Queiroz de Medeiros, "E-APK: Energy pattern detection in decompiled android applications," *J. Comput. Lang.*, vol. 76, no. May, p. 101220, 2023, doi: 10.1016/j.cola.2023.101220.

[20] G. Kale, G. E. Bostancı, and F. V. Çelebi, "Evolutionary feature selection for machine learning based malware classification," *Eng. Sci. Technol. an Int. J.*, vol. 56, no. July 2024, p. 101762, 2024, doi:

10.1016/j.jestch.2024.101762.

[21] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, “A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features,” *IEEE Access*, vol. 7, no. May, pp. 64411–64430, 2019, doi: 10.1109/ACCESS.2019.2916886.

[22] E. Chatzoglou, V. Kouliaridis, G. Kambourakis, G. Karopoulos, and S. Gritzalis, “A hands-on gaze on HTTP/3 security through the lens of HTTP/2 and a public dataset,” *Comput. Secur.*, vol. 125, p. 103051, 2023, doi: 10.1016/j.cose.2022.103051.

[23] K. Mahmud, S. Azam, A. Karim, S. Zobaed, B. Shanmugam, and D. Mathur, “Machine Learning Based PV Power Generation Forecasting in Alice Springs,” *IEEE Access*, vol. 9, pp. 46117–46128, 2021, doi: 10.1109/ACCESS.2021.3066494.

[24] G. Phillips *et al.*, “Setting nutrient boundaries to protect aquatic communities: The importance of comparing observed and predicted classifications using measures derived from a confusion matrix,” *Sci. Total Environ.*, vol. 912, no. July 2023, 2024, doi: 10.1016/j.scitotenv.2023.168872.