KLASIFIKASI *MALWARE ADWARE* PADA *ANDROID* MENGGUNAKAN METODE *SUPPORT VEKTOR MACHINE* (SVM) DAN *LINEAR DISCRIMINANT ANALYSIS* (LDA)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH:

PADHLI MAULANA
09011381722119

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2022

LEMBAR PENGESAHAN

KLASIFIKASI *MALWARE ADWARE* PADA *ANDROID* MENGGUNAKAN METODE *SUPPORT VEKTOR MACHINE* (SVM) DAN *LINEAR DISCRIMINANT ANALYSIS* (LDA)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH:

PADHLI MAULANA
09011381722119

Palembang, 25 Maret 2022

Pembimbing I	Pembimbing II
Ahmad Heryanto, S.Kom., M.T.	**Ahmad Fali Oklilas, M.T.**
NIP. 198701222015041002	**NIP. 197210151999031001**

Mengetahui, 4/4/22
Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis

Tanggal : 17 Maret 2022

Tim Penguji:

1. **Ketua Sidang** : **Dr. Ir. H. Sukemi, M.T.**
2. **Sekretaris Sidang** : **M. Ali Buchari, M.T.**
3. **Penguji Sidang** : **Kemahyanto Exaudi, M.T.**
4. **Pembimbing I** : **Ahmad Heryanto, M.T.**
5. **Pembimibing II** : **Ahmad Fali Oklilas, M.T.**

Mengetahui, 1/4/22
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda yangan dibawah ini:

Nama : Padhli Maulana

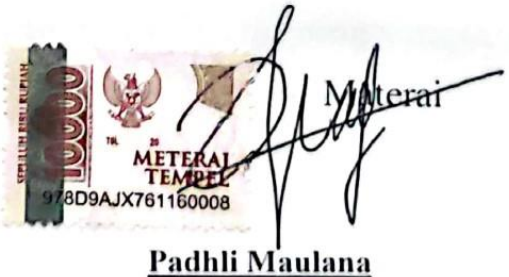
NIM : 09011381722119

Judul : KLASIFIKASI *MALWARE ADWARE* PADA *ANDROID* MENGGUNAKAN METODE *SUPPORT VEKTOR MACHINE* (SVM) DAN *LINEAR DISCRIMINANT ANALYSIS* (LDA)

Hasil pengecekan *Software iThentivate/Turnitin* : 7%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, Maret 2022



Meterai

Padhli Maulana
0901138172219

MOTTO DAN PERSEMBAHAN

Motto :

“Lelah Tidak Pernah Di Rasakan Oleh Mereka Yang Tidak Mau Berusaha”

“ Belajarlah kamu semua, dan mengajarlah kamu semua dan hormatilah guru-gurumu, serta belaku baiklah terhadap orang yang mengajarkanmu.”(HR Tabrani)

Persembahan:

Skripsi ini saya persembahkan untuk orang yang sangat berpengaruh didalam hidup saya, kedua orang tua. Keduanyalah yang membuat segalanya menjadi mungkin sehingga saya bisa ke tahap dimana saya bisa menyelesaikan skripsi saya hingga selesai. Terima kasih atas segala pengorbanan, nasehat, dan doa terbaik yang selalu engkau berikan padaku. Aku sangat bersyukur atas keberadaan kalian dalam kehidupanku.

KATA PENGANTAR

Assalamualikum Wr. Wb. Puji dan syukur saya hanturkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga saya dapat menyelesaikan penyusunan tugas Akhir ini dengan judul ‘‘Klasifikasi *Malware Adware* pada *Android* Menggunakan Metode *Support Vektor Machine* (SVM) dan *Linear Discriminant Analysis* (LDA)”.

Dalam tugas akhir ini penulis menjelaskan mengenai Klasifikasi *malware adware* pada *android* menggunakan metode *Support Vektor Machine* (SVM) dan *Linear Discriminant Analysis* (LDA), berserta dengan data-data hasil penelitian yang saya lakukan. Harapan saya agar tulisan ini dapat bermanfaat serta menjadi penambah wawasan bagi pembaca.

Pada penyusunan tugas akhir ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT dan terimakasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan kemudahan, kesehatan, serta kesempatan dalam pelaksanaan pembuatan Tugas Akhir ini.
2. Ibu, Ayah, Adik, serta Keluarga Besar saya yang telah memberikan dukungan dan nasehat serta motivasi selama ini. Terima kasih atas dukungan baik berupa moral, material, maupun spiritual.
3. Bapak Jaidan Jauhari, S.Pd., M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Kompuer Fakutas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Pembimbing I dan Bapak Ahmad Fali Oklilas, M.T. selaku Pembimbing II dan juga sebagai pembimbing Akademik di Jurusan Sistem Komputer.

6. Seluruh Dosen, Staff dan karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Teman-teman seperjuangan Sistem Komputer Angkatan 2017 Bukit yang selalu memberi dukungan.
8. Teman seperjuangan Kedal Squad.
9. Dan semua kerabat yang tidak dapat saya sebutkan satu persatu.

Tiada lain harapan saya semoga Allah SWT membalas segala niat baik kepada semua pihak yang saya sebutkan diatas. Saya menyadari bahwa proposal tugas akhir ini masih banyak kekurangan, oleh karena itu kritik serta saran yang membangun sangat saya harapkan sebagai bahan acuan dan perbaikan saya dalam menyempurnakan tugas akhir ini.

Semoga tugas akhir ini akan menjadi tambahan ilmu pengetahuan serta menambah wawasan kita dan memberi bermanfaat bagi semuanya. Sebelum dan sesudahnya penulis mengucapkan terimakasih.

Palembang, Maret 2022

Padhli Maulana

NIM. 09011381722119

KLASIFIKASI MALWARE ADWARE PADA ANDROID MENGGUNAKAN METODE SUPPORT VEKTOR MACHINE (SVM) DAN LINEAR DISCRIMINANT ANALYSIS (LDA)

PADHLI MAULANA (09011381722119)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Univesitas Sriwijaya
Email: padhlimaulana252@gmail.com

ABSTRAK

Internet merupakan penghubung antara satu media elektonik dengan media elektronik lainnya dengan cepat dan akurat dalam suatu jaringan komunikasi. Dimana jaringan komunikasi tersebut mengirimkan informasi yang ditransmisikan dengan memberi sinyal pada frekuensi yang disesuaikan[3]. *Adware* adalah perangkat lunak yang digunakan untuk menampilkan iklan untuk keuntungan moneter[6].. Dataset yang berasal dari *Canadian Institute for Cybersecurity* (CIC) dengan nama *android adware* 2017. Selain itu, ada metode *Linear Discriminant Analysis* (LDA) yang berfungsi sebagai reduksi dimensi data pada penelitian ini. Hasil dari klasifikasi *malware adware* menggunakan metode *Support Vektor Machine*(SVM) dan *Linear Discriminant Analysis* (LDA) adalah dengan menggunakan parameter RBF dengan nilai *range* terbesar yaitu *cost* = 32-250 dan *gamma* = 1 dengan hasil *accuracy* = 93,41%, *recall* = 79,5%, *precision* = 88,18%, *FPR* = 0,24%.

Kata Kunci *: Malware, internet, Android, klasifikasi, Support Vector Machine, Linear Discriminant Analysis*

CLASSIFICATION OF ADWARE MALWARE ON ANDROID USING SUPPORT VECTOR MACHINE (SVM) AND LINEAR DISCRIMINANT ANALYSIS (LDA) METHODS

PADHLI MAULANA (09011381722119)
Departement of Computer Engineering, Faculty of Computer Science,
Sriwijaya University
Email: padhlimaulana252@gmail.com

ABSTRACT

The internet is a liaison between one electronic media and other electronic media quickly and accurately in a communication network. Where the communication network sends information that is transmitted by signaling at an adjusted frequency[3]. *Adware is software that is used to display advertisements for monetary gain*[6]. *The dataset comes from the Canadian Institute for Cybersecurity (CIC) with the name android adware 2017. In addition, there is a Linear Discriminant Analysis (LDA) method that functions as a data dimension reduction in this study. The results of the adware malware classification using the Support Vector Machine (SVM) and Linear Discriminant Analysis (LDA) methods are to use the RBF parameter with a value of the largest is cost = 32-250 and gamma = 1 with accuracy = 93.41%, recall = 79.5%, precision = 88.18%, FPR = 0.24%..*

Keywords *: Malware, internet, Android, classification, Support Vector Machine, , Linear Discriminant Analysis*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1. Latar Belakang

Di zaman yang serba *modern*, teknologi sangat berkembang dengan pesat. Sehingga teknologi dapat ditemukan dimana saja. Bahkan teknologi tersebut banyak di gunakan dalam kehidupan sehari-hari. Salah satunya adalah teknologi yang tertanam didalam *smartphone* yaitu *android.*

Android adalah *System Operation* (SO) yang dibangun ke dalam *smartphone* [1]. *Android* menyediakan platform terbuka bagi pengembang untuk membangun aplikasi mereka sendiri [2]. *System Operation* (OS) sama dengan *Windows* dan *Apple* yang memiliki banyak fitur, kekuatan dan kelemahan. *Android* dapat memaksimalkan potensinya saat terhubung ke internet.

Internet merupakan penghubung antara satu media elektonik dengan media elektronik lainnya dengan cepat dan akurat dalam suatu jaringan komunikasi. Dimana jaringan komunikasi tersebut mengirimkan informasi yang ditransmisikan dengan memberi sinyal pada frekuensi yang disesuaikan[3]. Dengan adanya internet, *android* bisa di manfaatkan menjadi ladang bisnis yang bisa mempermudah sesorang untuk mendapatkan dana. Ada banyak cara untuk mendapatkan uang melalui internet, salah satu contohnya adalah dengan mempromosikan suatu produk dengan iklan.

Internet yang digunakan didalam *android* dengan cepat mengubah strategi pemasaran ke arah periklanan digital[4]. Iklan digital muncul saat Anda menjelajahi Internet atau menggunakan aplikasi *smartphone*. Sebagian besar *smartphone* saat ini menggunakan *platform Android*, sehingga ekosistem aplikasi *android* telah berkembang secara signifikan. Maraknya iklan digital juga memaksa *hacker* untuk menciptakan insentif untuk penipuan iklan. Perangkat lunak yang melakukan penipuan iklan

disebut *adware*[5].

Adware adalah perangkat lunak yang digunakan untuk menampilkan iklan untuk keuntungan moneter[6]. *Adware* juga dapat berisi bentuk aktivitas berbahaya lainnya. Misalnya, *adware* dapat dikonfigurasi untuk mencuri informasi rahasia dari *smartphone* pengguna dan menyebarkannya ke pihak ketiga[5].

Untuk mengklasifikasi *malware adware*, ada banyak metode yang diterapkan pada penelitian sebelumnya seperti metode *random forest*[7], *Adaboost*[8]. Terdapat juga metode *support vector machine* (SVM) dan *Linear Discriminant Analysis* (LDA) yang di terapkan dalam mengklasifikasi hewan yaitu anjing dan kucing[9]. Sehingga peneliti akan menerapkan metode *support vector machine* (SVM) dan *Linear Discriminant Analysis* (LDA) dalam mengklasifikasi *malware adware* dan *benign*.

SVM merupakan teknik klasifikasi dengan tujuan untuk menemukan *hyperplane* dari banyak kelas yang berbeda dengan memisahkan banyak kumpulan data[10]. SVM memiliki keunggulan dalam penentuan jarak sehingga proses perhitungannya cepat. SVM adalah metode klasifikasi yang memiliki proses pelatihan yang efisien dan dapat dioptimalkan di semua area percobaan. Dan sebagai pereduksi data menggunakan *Linear Discriminant Analysis* (LDA).

Linear Discriminant Analysis (LDA) adalah algoritma yang menggunakan teori statistik dalam pembelajaran mesin, pemrosesan data, dan pemrosesan gambar. Algoritma ini dikembangkan dan dipublikasikan pertama kali oleh Ronald A. Fisher pada tahun 1936 dalam artikel *The Use of Multiple Measures in Taxonomic Problems*. LDA merupakan algoritma ekstraksi fitur dengan kombinasi perhitungan operasi matematika dan statistik menggunakan properti statistik terpisah untuk setiap objek[11].

Tujuan dari dilakukannya penelitian ini dalam mengklasifikasi *malware adware* pada *android* adalah seberapa besar akurasi yang akan dihasilkan dengan menggunakan metode *support vector machine* (SVM) dan *Linear Discriminant Analysis* (LDA).

1.2. Perumusan Masalah

Berdasarkan penjelasan pada bagian latar belakang diatas, rumusan masalah yang diambil adalah:

1. Bagaimana mengklasifikasi data *adware* dan *benign*?
2. Bagaimana menerapkan metode *support vector machine*(SVM) dan *Linear Discriminant Analysis* (LDA)?
3. Bagaimana menerapkan Dataset yang berasal dari *Canadian Institute for Cybersecurity* (CIC) bernama android adware untuk mengklasifikasi *malware adware*?

1.3. Batasan Masalah

Batasan masalah yang diterapkan pada penelitian ini, antara lain:

1. Pengklasifikasian hanya *malware Adware* dan *benign*..
2. Metode yang diterapkan adalah *support vector machine*(SVM) dan *Linear Discriminant Analysis* (LDA).
3. *Dataset* yang digunakan berasal dari *Canadian Institute for Cybersecurity* (CIC) dengan nama *android adware* 2017.

1.4. Tujuan

Adapun tujuan yang dilakukan pada penelitian ini adalah:

1. Menerapkan metode *Linear Discriminant Analysis* (LDA) pada dataset yang berasal dari *Canadian Institute For Cybersecurity* (CIC) dengan nama *android adware 2017*.
2. Menerapkan parameter *Radial Basis Function* (RBF) pada metode SVM .
3. Menganalisis hasil dari klasifikasi *malware adware* menggunakan metode *support vector machine*(SVM) dan *Linear Discriminant Analysis* (LDA).

1.5. Manfaat

Adapun manfaat yang dilakukan dalam penelitian ini adalah:

1. Dapat mempelajari proses dalam klasfikasi *malware adware*.
2. Bisa menjadi bahan referensi.
3. Bisa mengklasifikasikan data *malware adware* dan *benign*.

1.6. Metodologi Penelitian

Ada beberapa tahapan metologi dalam melakukan penelitian ini. Tahap ini adalah penentuan pokok permasalahan mengenai klasifikasi *adware android*.

1. Tahap study pustaka (*literature*)

   Dalam tahapan ini penulis mengambil jurnal dan buku untuk mencari referensi sebagai acuan dalam menyelesaikan rumusan masalah yang berkaitan dengan metode penelitian.

2. Tahap perancangan

   Dalam tahapan ini penulis melakukan perancangan dalam penelitian berlandaskan *literatur* dan rumusan masalah yang digunakan.

3. Tahap pengujian

   Dalam tahapan ini penulis melakukan mengujian *source code* dan algoritma yang telah di buat untuk mendapatkan hasil akurasi dalam mengklasfikasi *malware adware*.

4. Tahap analisisa

   Dalam tahapan ini penulis melakukan pengambilan dan menganalisa data sehingga mendapatkan hasil akurasi dalam mengklasifikasi *malware adware* berdasarkan *source code* dan algoritma yang di buat.

5. Kesimpulan dan saran

   Dalam tahapan ini penulis mengambil kesimpulan serta analisa dan memberi saran Sistematika untuk penulis selanjutnya.

6. Penulisan

Adapun sistematika penulisan yang di terapkan pada penelitian ini adalah:

BAB I PENDAHULUAN

Bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi penelitian, dan sistematika penulisan yang akan di gunakan dalam laporan penelitian ini.

BAB II TIJAUAN PUSTAKA

Bab ini menjelaskan tentang teori-teori yang bertautan dengan masalah *malware adware* dengan metode *support vector machine* (SVM) dan *Linear Discriminant Analysis* (LDA).

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang kerangka kerja penelitian, perancangan sistem, dan pengujian.

BAB IV HASIL DAN ANALISIS

Bab ini menjelaskan tentang hasil dan analisa terhadap penelitian yang telah dilakukan mengenai klasifikasi malware adware pada andorid menggukan metode *support vector machine*(SVM) dan *Linear Discriminant Analysis* (LDA).

BAB V KESIMPULAN

Pada bab ini menjelaskan tentang bagaimana menyimpulkan dari penelitian yang di lakukan berdasar analisa .

DAFTAR PUSTAKA

[1] A. Fatoni, D. B. Rendra, P. Studi, S. Komputer, and I. Pendahuluan, "PERANCANGAN PROTOTYPE SISTEM KENDALI LAMPU MENGGUNAKAN HANDPHONE ANDROID," vol. 1, no. September, 2014.

[2] K. Khairul, S. Haryati, and Y. Yusman, "Aplikasi Kamus Bahasa Jawa Indonesia Dengan Algoritma Raita Berbasis Android," *J. Teknol. Inf. dan Pendidik.*, vol. 11, no. 1, pp. 1–6, 2018, doi: 10.24036/tip.v11i1.102.

[3] . N., A. Ibrahim, and A. Ambarita, "Sistem Informasi Pengaduan Pelanggan Air Berbasis Website Pada Pdam Kota Ternate," *IJIS - Indones. J. Inf. Syst.*, vol. 3, no. 1, 2018, doi: 10.36549/ijis.v3i1.37.

[4] A. Tyas and D. Aryani, "Efektivitas Iklan Digital Google Adsense," *J. Ekon. dan Bisnis*, vol. 20, no. 1, pp. 19–28, 2017, [Online]. Available: https://jurnal.unikal.ac.id/index.php/jebi/article/view/689.

[5] 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, 2019, doi: 10.1007/s11416-018-0328-8.

[6] J. Y. Ndagi and J. K. Alhassan, "Machine learning classification algorithms for adware in android devices: A comparative evaluation and analysis," *2019 15th Int. Conf. Electron. Comput. Comput. ICECCO 2019*, no. Icecco, 2019, doi: 10.1109/ICECCO48375.2019.9043288.

[7] K. Lee and H. Park, *Malicious Adware Detection on Android Platform using Dynamic Random Forest*, vol. 994. Springer International Publishing, 2020.

[8] S. Suresh, "Analyzing Android Adware," 2018.

[9] A. Suryadibrata and S. D. Salim, "Klasifikasi Anjing dan Kucing menggunakan Algoritma Linear Discriminant Analysis dan Support Vector Machine," *Ultim. J. Tek. Inform.*, vol. 11, no. 1, pp. 46–51, 2019, doi: 10.31937/ti.v11i1.1076.

[10] S. Herlambang, S. Basuki, D. R. Akbi, and Z. Sari, "Deteksi Malware Android Berdasarkan System Call Menggunakan Algortima Support Vector Machine," vol. 5, pp. 157–165, 2015.

[11] S. Cahyani, R. Wiryasaputra, and R. Gustriansyah, "Identifikasi Huruf Kapital Tulisan Tangan Menggunakan Linear Discriminant Analysis dan Euclidean Distance," *J. Sist. Inf. Bisnis*, vol. 8, no. 1, p. 57, 2018, doi: 10.21456/vol8iss1pp57-67.

[12] M. Alkaff, A. R. Baskara, and I. Maulani, "Klasifikasi Laporan Keluhan Pelayanan Publik Berdasarkan Instansi Menggunakan Metode LDA-SVM," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 8, no. 6, p. 1265, 2021, doi: 10.25126/jtiik.2021863768.

[13] M. F. Fibrianda and A. Bhawiyuga, "Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. II, no. 9, pp. 3112–3123, 2018.

[14] R. Mirzazadeh, M. H. Moattar, and M. V. Jahan, "Metamorphic malware

detection using Linear Discriminant Analysis and Graph Similarity," *2015 5th Int. Conf. Comput. Knowl. Eng. ICCKE 2015*, no. October, pp. 61–66, 2015, doi: 10.1109/ICCKE.2015.7365862.
[15] I. Martín, J. A. Hernández, and S. de los Santos, "Machine-Learning based analysis and classification of Android malware signatures," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 295–305, 2019, doi: 10.1016/j.future.2019.03.006.
[16] I. M. M. Matin and B. Rahardjo, "Malware Detection Using Honeypot and Machine Learning," *2019 7th Int. Conf. Cyber IT Serv. Manag. CITSM 2019*, 2019, doi: 10.1109/CITSM47753.2019.8965419.
[17] S. I. Imtiaz, S. ur Rehman, A. R. Javed, Z. Jalil, X. Liu, and W. S. Alnumay, "DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network," *Futur. Gener. Comput. Syst.*, vol. 115, pp. 844–856, 2021, doi: 10.1016/j.future.2020.10.008.
[18] A. I. Elkhawas and N. Abdelbaki, "Malware Detection using Opcode Trigram Sequence with SVM," *2018 26th Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2018*, pp. 7–11, 2018, doi: 10.23919/SOFTCOM.2018.8555738.
[19] T. Tuncer, F. Ertam, and S. Dogan, "Automated malware identification method using image descriptors and singular value decomposition," *Multimed. Tools Appl.*, vol. 80, no. 7, pp. 10881–10900, 2021, doi: 10.1007/s11042-020-10317-6.
[20] Ferdiansyah, "Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware," *JUSIFO (Jurnal Sist. Informasi)*, vol. 2, no. 1, pp. 44–59, 2018, [Online]. Available: http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue dan Wannacry Ransomware.pdf.
[21] L. K. Hatika, A. Budiyono, A. Almaarif, F. R. Industri, and U. Telkom, "ANALISIS KETEPATAN DETEKSI MALWARE PADA SOFTWARE ANTIVIRUS MENGGUNAKAN METODE ANALISIS STATIS ACCURACY ANALYSIS OF MALWARE DETECTION IN ANTIVIRUS SOFTWARE," vol. 6, no. 2, pp. 7812–7819, 2021.
[22] L. Mathur, M. Raheja, and P. Ahlawat, "Botnet Detection via mining of network traffic flow," *Procedia Comput. Sci.*, vol. 132, pp. 1668–1677, 2018, doi: 10.1016/j.procs.2018.05.137.
[23] N. S. Tajriyani, "Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran Ransomware Cryptolocker," *Jurist-Diction*, vol. 4, no. 2, p. 685, 2021, doi: 10.20473/jd.v4i2.25785.
[24] Z. Liu, J. Ye, X. Hu, H. Li, X. Li, and Y. Hu, "Sequence Triggered Hardware Trojan in Neural Network Accelerator," *Proc. IEEE VLSI Test Symp.*, vol. 2020-April, pp. 0–5, 2020, doi: 10.1109/VTS48691.2020.9107582.
[25] R. L. Putra, "Analisis Aktivitas Malware Pada Ram Android Dan Sandbox Environment," 2019.
[26] Hestylesta, "Bab ii teori penunjang 2.1 umum," no. September 2015, pp. 6–

26, 2009.
[27] S. D. S. K. Virgiawan A. Manoppo, Arie S. M. Lumenta, “Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi,” *J. Tek. Elektro Dan Komput.*, vol. 9, no. 3, pp. 181–188, 2020.
[28] C. Gutzman, S. Sweep, and A. Tambo, “Differences and similarities of spyware and adware,” *Univ. Minnesota Morris*, 2003, [Online]. Available: file:///Users/atb/Documents/Library.papers3/Files/2003 Gutzman.pdf%5Cnpapers3://publication/uuid/AE9873B9-9EA3-4C37-91CF-AC13ECACA9BF.
[29] F. M. Hana, “Perbandingan Algoritma Neural Network Dengan Linier Discriminant Analysis (Lda) Pada Klasifikasi Penyakit Diabetes,” vol. 1, pp. 1541–1541, 2020.
[30] R. Mirzazadeh, M. H. Moattar, and M. V. Jahan, “Metamorphic malware detection using Linear Discriminant Analysis and Graph Similarity,” *2015 5th Int. Conf. Comput. Knowl. Eng. ICCKE 2015*, pp. 61–66, 2015, doi: 10.1109/ICCKE.2015.7365862.
[31] D. A. Pramudita and A. Musdholifah, “GSA to Obtain SVM Kernel Parameter for Thyroid Nodule Classification,” *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 14, no. 1, p. 11, 2020, doi: 10.22146/ijccs.41215.
[32] “Universitas Sumatera Utara,” 2018.
[33] Fadli, “Preeklampsia Universitas Sumatera Utara,” *Preeklamsia Berat*, pp. 44–85, 2018, [Online]. Available: repository.usu.ac.id/bitstream/123456789/30230/4/Chapter II.pdf.
[34] L. K. Ramasamy, S. Kadry, and S. Lim, “Selection of optimal hyper-parameter values of support vector machine for sentiment analysis tasks using nature-inspired optimization methods,” *Bull. Electr. Eng. Informatics*, vol. 10, no. 1, pp. 290–298, 2021, doi: 10.11591/eei.v10i1.2098.
[35] A. C. Florea and R. Andonie, “A dynamic early stopping criterion for random search in SVM hyperparameter optimization,” *IFIP Adv. Inf. Commun. Technol.*, vol. 519, pp. 168–180, 2018, doi: 10.1007/978-3-319-92007-8_15.
[36] W. Jiang and S. Siddiqui, “Hyper-parameter optimization for support vector machines using stochastic gradient descent and dual coordinate descent,” *EURO J. Comput. Optim.*, vol. 8, no. 1, pp. 85–101, 2020, doi: 10.1007/s13675-019-00115-7.
[37] D. Istiawan and L. Khikmah, “Implementation of C4.5 Algorithm for Critical Land Prediction in Agricultural Cultivation Areas in Pemali Jratun Watershed,” *Indones. J. Artif. Intell. Data Min.*, vol. 2, no. 2, p. 67, 2019, doi: 10.24014/ijaidm.v2i2.7569.