KLASIFIKASI ADWARE DENGAN *PRINCIPAL COMPONENT ANALYSIS* (PCA) MENGGUNAKAN *RANDOM FOREST*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

RIZKY MARLIANSYAH

09011381722112

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

LEMBAR PENGESAHAN

KLASIFIKASI ADWARE DENGAN *PRINCIPAL COMPONENT ANALYSIS* (PCA) MENGGUNAKAN RANDOM FOREST

SKRIPSI

Program Studi Sistem Komputer
Jenjang S1

Oleh :

RIZKY MARLIANSYAH
09011381722112

Palembang, 19 Juli 2022

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Skripsi
Dr. Ir. H. Sukemi, M.T.	Ahmad Heryanto, S.Kom., M.T
NIP. 196612032032006041001	NIP. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Jumat

Tanggal : 29 Juli 2022

Tim Penguji :

1. **Ketua Sidang** : **Ahmad Zarkasi, M.T.**
2. **Sekretaris Sidang** : **Adi Hermansyah, M.T.**
3. **Penguji Sidang** : **Ahmad Fali Oklilas, M.T.**
4. **Pembimbing** : **Ahmad Heryanto, M.T.**

Mengetahui

Ketua Jurusan Sistem Komputer

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

NIP 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda yangan dibawah ini:

Nama : Rizky Marliansyah

NIM : 09011381722112

Judul : KLASIFIKASI ADWARE DENGAN *PRINCIPAL COMPONENT ANALYSIS (PCA)* MENGGUNAKAN *RANDOM FOREST*

Hasil pengecekan *Software iThentivate/Turnitin* : 6%

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 ada paksaan.

Palembang, 29 Juli 2022

Rizky Marliansyah

09011381722112

MOTTO :

TUHAN TAK PERNAH MEMBERI UJIAN DIATAS KEMAMPUAN UMATNYA, MAKA DARI ITU KITA SEBAGAI UMATNYA HARUS MENSYUKURI DI SETIAP KEADAAN BAIK ITU SUKA MAUPUN DUKA KARNA KITA TIDAK AKAN PERNAH TAU KAPAN IA AKAN DATANG.

DISAAT TERPURUK, ITULAH MOMEN YANG PAS UNTUK MENUNJUKKAN SIAPA DIRIMU SEBENARNYA DAN MULAI LAH UNTUK BANGKIT JANGAN KALAH OLEH KEADAAN.

NEVER GIVE UP !

DISAAT KAMU MEMPUNYAI SEGALANYA, COBALAH UNTUK MENGINGAT SEBERAPA SULITNYA KAMU BANGKIT DARI KEADAAN TERPURUK.

BE HUMBLE !

KATA PENGANTAR

Alhamdulillah dan puji syukur penulis panjatkan atas kehadirat Allah SWT, dengan segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penelitian tugas akhir yang berjudul **" Klasifikasi Adware Dengan *Principal Component Analysis* (PCA) Menggunakan Random Forest "**.

Penulisan Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan proposal ini. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Proposal Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. Dan tak lupa mengucapkan terima kasih kepada yang terhormat :

1. Kedua Orang Tua saya terutama ibunda saya tercinta yang selalu mensupport serta mendoakan saya sehingga saya sebagai penulis mampu menempuh perjalan pendidikan sehingga bisa mengikuti dan melaksanakan perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya hingga dapat menyelesaikan tugas akhir ini.
2. Seluruh Keluarga Besar Hj. Rahuna yang telah mensupport moral dan materi bagi penulis.
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 Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, M.T. selaku Dosen Pembimbing Tugas Akhir penulis.

6. Bapak Dr. Erwin, S.Si, M.Si selaku Dosen Pembimbing Akademik penulis.
7. Dosen, staff, serta seluruh karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Teruntuk Tata Satria Timor Perdana dan Fidya Rianti Putri sebagai partner bagi penulis.
9. Kak Nabilah Humairah yang telah membantu penulis dalam dunia perkuliahan.
10. Seluruh teman-teman yang ada di grup SK2017 sekeluarga, meliputi Nawawi, Barzan, Hadi, Hafizd, Kincai, Baduz, Azan, Ferdiyon, Ardi, Yuan, dan Ardani.
11. Seluruh teman angkatan 2017 Sistem Komputer bukit.
12. Seluruh teman dan keluarga 50NG Fams.
13. Seluruh teman-teman yang berada didalam grup 19seconds, RRQ MDL, Calavera, meliputi Eko, Arief, Amet, Aldi, Zahir, Bayu, dan juga Mufti.
14. Dan yang terakhir, terima kasih kalian barisan para mantan dan semua yang pergi tanpa sempat aku miliki.
15. Almamater Unsri tercinta.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Tugas Akhir ini. Karena sesungguhnya tak ada yang sempurna didunia ini. Untuk itu, segala saran dan kritik sangatlah penting bagi penulis. Akhir kata, semoga penelitian Tugas Akhir ini dapat bermanfaat dan berguna bagi khalayak.

Palembang, Juli 2022

Penulis

Rizky Marliansyah

NIM. 0911381722112

Abstrak

KLASIFIKASI ADWARE DENGAN *PRINCIPAL COMPONENT ANALYSIS* (PCA) MENGGUNAKAN *RANDOM FOREST*

Rizky Marliansyah (09011381722112)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : rizkymrl30@gmail.com

Abstrak

Algoritma ekstraksi dan pemilihan fitur yang tidak diawasi, yang banyak digunakan untuk melakukan tugas pengurangan dimensi untuk menghindari overfitting. Machine Learning yaitu merupakan system pembelajaran mesin dalam pendekatan system kecerdasan buatan atau Artificial Intelligence dengan simulasi dari kecerdasan yang dimiliki oleh manusia yang dimodelkan di dalam mesin dan diprogram agar bisa berpikir seperti halnya manusia. Pada penelitian ini dijelaskan berhasil menggunakan klasifikasi Adware menggunakan Random Forest dan kali ini akan mengunakan algoritma dari Principal Componen Analysis (PCA) yang berfungsi sebagai proses reduksi dimensi pada data yang digunakan. Dari penelitian tersebut hasil yang didapatkan dari komponen pun cukup baik dengan nilai akurasi 98,85%. Sedangkan nilai recall sebesar 98,34% lalu nilai presisi 98,52% dan nilai FPR 0,44% serta OOB-error 1,05%.

Kata Kunci : *Machine Learning*, Klasifikasi, *Adware*, Algoritma *PCA*, *Random Forest*.

Mengetahui, 05/11/22

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T

NIP. 196612032032006041001

Dosen Pembimbing

Ahmad Heryanto, M.T

NIP. 198701222015041002

Abstract

ADWARE CLASSIFICATION WITH PRINCIPAL COMPONENT ANALYSIS (PCA) USING RANDOM FOREST

Rizky Marliansyah (09011381722112)

Department of Computer Engineering, Faculty of Computer Science, Sriwijaya University

Email : rizkymrl30@gmail.com

Abstract

Unsupervised feature extraction and selection algorithms, which are widely used to perform dimensionality reduction tasks to avoid overfitting. Machine Learning is a machine learning system in an artificial intelligence system approach or Artificial Intelligence with a simulation of the intelligence possessed by humans which is modeled in machines and programmed to think like humans. In this study, it is explained that the Adware classification using Random Forest is successful and this time it will use the algorithm from Principal Component Analysis (PCA) which functions as a dimension reduction process in the data used. From this research, the results obtained from the components are quite good with an accuracy value of 98.85%. While the recall value is 98.34%, the precision value is 98.52% and the FPR value is 0.44% and the OOB-error is 1.05%.

Keywords : *Machine Learning, Classfication, Adware, Algorithm PCA, Random Forest.*

Knowing, 27/11/22

Ketua Jurusan Sistem Komputer	**Dosen Pembimbing**
Dr. Ir. H. Sukemi, M.T	**Ahmad Heryanto, M.T**
NIP. 196612032006041001	**NIP. 198701222015041002**

ix

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi secara tidak langsung memberikan tantangan dan ancaman bagi pengguna internet, tingginya tingkat penyebaran internet berdampak dalam tingkat kejahatan, baik itu di dunia maya ataupun dunia nyata. Salah satu bentuk kejahatan di dunia maya disebut juga *cyber crime* adalah pencurian data secara ilegal.

Banyaknya aktifitas penyebaran malware yang terjadi melalui jaringan internet membuat banyak pengguna menjadi resah salah satu bentuk dari serangan tersebut yaitu dengan melakukan penyisipan file-file berbahaya atau malicious ke komputer. Contohnya seperti penyisipan skrip *web shell* yang di sisipkan ke komputer penyedia layanan internet.[1]

Kerangka kerja Android API berisi fungsi untuk mengakses sumber daya sensitif dalam sistem. Hal ini memungkinkan penyerang dunia maya untuk membuat aplikasi jahat dan mendistribusikannya melalui toko aplikasi pihak ketiga atau iklan melalui jejaring sosial.[2]

Malware ini salah satu jenis perangkat lunak apa pun yang dibuat dengan tujuan mencuri atau mendapatkan informasi sensitifitas dari seseorang. Mereka memiliki kemampuan untuk meniru mesin. Malware juga merupakan sebuah rancangan dari perangkat lunak yang bisa menyusup ke sebuah system operasi yang bersifat dapat mengganggu system dan merusak ataupun mencuri beberapa arsip data yang penting didalam system tersebut. Banyak oknum yang memanfaatkan malware sebagai system penerimaan data data penting para korban dengan tujuan tertentu. Tipikal smartphone yang menggunakan jenis system operasi android juga rentan menjadi sasaran empuk bagi para oknum tersebut. Dimana pada malware tersebut dapat merusak system android melalui beberapa iklan yang terdapat pada aplikasi yang dijalankan ataupun juga pada jenis website yang telah kita telusuri serta

menyebar di berbagai seluruh jaringan yang telah kita lakukan menjadi sangat berbahaya.[3]

Ancaman *malware* terus berkembang secara vertikal (yaitu jumlah dan volume) dan horizontal (yaitu jenis dan fungsionalitas) karena peluang yang diberikan oleh kemajuan teknologi. Internet, jejaring sosial, *smartphone*, perangkat IoT, dan sebagainya, memungkinkan terciptanya *malware* yang cerdas dan canggih.[4]

Algoritma ekstraksi dan pemilihan fitur yang tidak diawasi, yang banyak digunakan untuk melakukan tugas pengurangan dimensi untuk menghindari *overfitting*. Mengingat ruang fitur asli, PCA menemukan proyeksi linier dirinya sendiri di ruang dimensi yang lebih rendah yang ingin dicapai.[5]

Teknik klasifikasi seperti *Support Vector Machines, K-Nearest Neighbours, Decision Trees, Logistic Regression,* dan *Naive Bayes* telah banyak digunakan di dalam penelitian deteksi intrusi di komunitas keamanan. Terutama digunakan untuk metode deteksi berbasis perilaku, juga disebut metode deteksi anomali. untuk mengidentifikasi kelayakan penggunaan klasifikasi *Random Forest* untuk mendeteksi jika perangkat Android telah disusupi oleh *malware* dengan memeriksa data perilaku aplikasi.[6]

Beberapa algoritma yang temasuk dalam Supervised Learning telah memiliki hasil hasil tertentu dalam setiap pengujian data. Dimana pada setiap data hamper memiliki tingkat hasil pengujian yang berbeda beda dengan memanfaatkan system dari algoritma tersebut. [7]

Pada penelitian sebelumnya[8], telah dilakukan Klasifikasi Android Malware yang menggunakan beberapa metode yakni Random Forest, Decision Tree (DT) dan K-Nears Nighbor (KNN). Akan tetapi dataset yang digunakan sudah kuno. Dari penelitian tersebut didapatlah hasil terbaik yaitu dengan menggunakan algoritma Random Forest. Nilai recall yang didapat adalah 88.30%, sedangkan untuk nilai presisi-nya adalah 85.80%.

Dalam pembahasan penelitian sebelumnya agar mendapatkan hasil yang lebih efektif, maka penulis berusaha meng implementasikan algoritma

Random Forest dalam mengklasifikasikan *Android Malware* berjenis *Adware* dan menggunakan dataset dari *CICAndMal2017*.

1.2 Tujuan

Adapun tujuan yang hendak dicapai dari hasil penelitian ini adalah :

1. Untuk mengimplementasikan *Principal Component Analysis* (PCA) dalam klasifikasi *Adware* dengan metode *Random Forest.*
2. Menganalisa terhadap hasil dari klasifikasi menggunakan algoritma *Random Forest* tanpa diterapkan reduksi dimensi.
3. Menganalisa terhadap hasil dari klasifikasi menggunakan algoritma *Random Forest* yang telah diterapkan algoritma *Principal Component Analysis* (PCA) sebagai reduksi dimensi.

1.3 Manfaat

Adapun manfaat yang diharapkan dapat diambil dari penelitian ini adalah :

1. Dapat mempelajari proses penyederhanaan data tanpa mengurangi parameter penting dalam data tersebut
2. Dapat memperoleh tingkat akurasi dalam proses klasifikasi adware

1.4 Perumusan dan Batasan Masalah

Adapun rumusan masalah pada penelitian ini antara lain :

1. Bagaimana penerapan proses PCA yang digunakan dalam meningkatkan efektifitas kinerja pengklasifikasian adware dengan metode Random Forest?

Adapun beberapa batasan dari masalah dalam penelitian ini antara lain :

1. Dataset yang dipakai dalam penelitian ini adalah data malware Android bertipe adware dalam dataset CICAndMal2017.
2. Mengklasifikasikan adware menggunakan *Principal Component Analysis* (PCA).
3. Metode yang digunakan adalah metode *random forest.*
4. *Dataset* yang digunakan dalam penelitian ini menggunakan format csv.

5. Proses pengklasifikasian ini dilakukan secara offline, bukan secara realtime.

1.5 Metodologi Penelitian

Adapun metodologi yang digunakan dalam penelitian ini akan melewati beberapa tahap, yaitu :

1. Tahap Pertama (Studi Pustaka/ Literatur)

Tahap ini dilakukan setelah masalah yang akan dibahas telah sesuai dan relevan untuk dijadikan sebagai penelitian, dengan mambaca artikel atau makalah penelitian yang berhubungan langsung dengan tugas akhir.

2. Tahap Kedua (Perancangan Sistem)

Tahap ini membahas mengenai proses bagaimana membangun system dengan menggunakan metode atau pendekatan tertentu, apa saja perangkat keras atau perangkat lunak yang digunakan, kemudian bagaimana proses instalasi dan konfigurasi sistem, selanjutnya bagaimana pula penerapan metode pada penelitian tugas akhir.

3. Tahap Ketiga (Pengujian)

Tahap ini merupakan tahap lanjutan dari proses perancangan yang telah dilakukan. Dengan melakukan pengujian berdasarkan metodologi penelitian dan penelitian sebelumnya sehingga didapatkan data hasil uji yang sesuai dan tepat dengan algoritma.

4. Tahap Keempat (Analisa)

Data yang diperoleh dari proses pengujian, kemudian dianalisis berdasarkan pendekatan tertentu, sehingga didapatkan hasil data yang objektif dimana data diperoleh dari hasil pengujian.

5. Tahap kelima (Kesimpulan dan Saran)

Pada tahap ini adalah membuat kesimpulan dari permasalahan, studi pustaka, metodologi, dan analisa hasil pengujian serta membuat beberapa saran yang dapat dijadikan penelitian selanjutnya.

DAFTAR PUSTAKA

[1] I. Anggraini and Y. N. Kunang, ‘Telematika Penerapan Naïve Bayes pada Pendeteksian Malware dengan Diskritisasi Variabel’, vol. 13, no. 1, pp. 11–21, 2020.

[2] R. Surendran, T. Thomas, and S. Emmanuel, ‘A TAN based hybrid model for android malware detection’, *J. Inf. Secur. Appl.*, vol. 54, p. 102483, 2020, doi: 10.1016/j.jisa.2020.102483.

[3] S. A. Roseline, ‘Forest Paradigm’, *2018 Int. Conf. Adv. Comput. Commun. Informatics*, pp. 330–336, 2018.

[4] D. Gibert, C. Mateu, and J. Planes, ‘The rise of machine learning for detection and classification of malware: Research developments, trends and challenges’, *J. Netw. Comput. Appl.*, vol. 153, no. July 2019, p. 102526, 2020, doi: 10.1016/j.jnca.2019.102526.

[5] C. D. Morales-molina, D. Santamaria-guerrero, G. Sanchez-perez, K. Toscano-medina, H. Perez-meana, and A. Hernandez-suarez, ‘Methodology for Malware Classification using a Random Forest Classifier’, *2018 IEEE Int. Autumn Meet. Power, Electron. Comput.*, no. Ropec, pp. 1–6, 2018.

[6] M. S. Alam and S. T. Vuong, ‘Random forest classification for detecting android malware’, *Proc. - 2013 IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Soc. Comput. GreenCom-iThings-CPSCom 2013*, pp. 663–669, 2013, doi: 10.1109/GreenCom-iThings-CPSCom.2013.122.

[7] D. Ucci, L. Aniello, and R. Baldoni, ‘Survey of machine learning techniques for malware analysis’, *Comput. Secur.*, vol. 81, pp. 123–147, 2019, doi: 10.1016/j.cose.2018.11.001.

[8] A. H. Lashkari, A. F. A. Kadir, L. Taheri, and A. A. Ghorbani, ‘Toward Developing a Systematic Approach to Generate Benchmark Android Malware Datasets and Classification’, *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2018-Octob, no. Cic, pp. 1–7, 2018, doi: 10.1109/CCST.2018.8585560.

[9] I. Z. Yadi and Y. N. Kunang, ‘Konferensi Nasional Ilmu Komputer (KONIK) 2014 Analisis Forensik Pada Platform Android’, *Konf. Nas. Ilmu Komput.*, p. 142, 2014, [Online]. Available: http://eprints.binadarma.ac.id/2191/.

[10] G. Dini, F. Martinelli, A. Saracino, and D. Sgandurra, 'MADAM: A multi-level anomaly detector for android malware', *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7531 LNCS, pp. 240–253, 2012, doi: 10.1007/978-3-642-33704-8_21.

[11] M. K. Alzaylaee, S. Y. Yerima, and S. Sezer, 'Computers & Security DL-Droid : Deep learning based android malware detection using real devices', vol. 89, 2020, doi: 10.1016/j.cose.2019.101663.

[12] J. Y. Ndagi and J. K. Alhassan, 'Machine Learning Classification Algorithms for Adware in Android Devices : A Comparative Evaluation and Analysis', no. Icecco, 2019.

[13] B. Amos, H. Turner, and J. White, 'Applying machine learning classifiers to dynamic android malware detection at scale', *2013 9th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2013*, pp. 1666–1671, 2013, doi: 10.1109/IWCMC.2013.6583806.

[14] B. Warf, 'Adware', *SAGE Encycl. Internet*, 2018, doi: 10.4135/9781473960367.n7.

[15] I. Ideses and A. Neuberger, 'Adware detection and privacy control in mobile devices', *2014 IEEE 28th Conv. Electr. Electron. Eng. Isr. IEEEI 2014*, 2014, doi: 10.1109/EEEI.2014.7005849.

[16] S. Suresh, F. Di, T. Katerina, and P. Mark, '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.

[17] F. C. C. Garcia and F. P. Muga, 'Random Forest for Malware Classification', pp. 1–4, 2016, [Online]. Available: http://arxiv.org/abs/1609.07770.

[18] A. Ahmad, 'Mengenal Artificial Intelligence, Machine Learning, Neural Network, dan Deep Learning', *Teknol. Indones.*, no. June, pp. 1–6, 2017.

[19] F. Livingston, 'Implementation of Breiman ' s Random Forest Machine Learning Algorithm', pp. 1–13, 2005.

[20] J. Burrell, 'How the machine "thinks": Understanding opacity in machine learning algorithms', *Big Data Soc.*, vol. 3, no. 1, pp. 1–12, 2016, doi: 10.1177/2053951715622512.

[21] B. S. Sasikala, V. G. Biju, and C. M. Prashanth, ‘Kappa and accuracy evaluations of machine learning classifiers’, *RTEICT 2017 - 2nd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. Proc.*, vol. 2018-Janua, pp. 20–23, 2017, doi: 10.1109/RTEICT.2017.8256551.

[22] G. Rahayu and M. Mustakim, ‘Principal Component Analysis Untuk Dimensi Reduksi Data Clustering Sebagai Pemetaan Persentase Sertifikasi Guru Di Indonesia’, *Semin. Nas. Teknol. Inf. Komun. dan Ind.*, vol. 0, no. 0, pp. 201–208, 2017, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/SNTIKI/article/view/3265.

[23] A. Izzuddin, ‘Optimasi Cluster pada Algoritma K-Means dengan Reduksi Dimensi Dataset Menggunakan Principal Component Analysis untuk Pemetaan Kinerja Dosen’, *Ed. Nop.*, vol. 5, no. 2, pp. 41–46, 2015.

[24] D. Tanta, C. Sirait, and W. Astuti, ‘Analisis Perbandingan Reduksi Dimensi Principal Component Analysis (PCA) dan Partial Least Square (PLS) untuk Deteksi Kanker menggunakan Data Microarray Pendahuluan Studi Terkait’, vol. 6, no. 2, pp. 8570–8581, 2019.

[25] S. R. Tiwari and R. U. Shukla, ‘An Android Malware Detection Technique Using Optimized Permission and API with PCA’, *Proc. 2nd Int. Conf. Intell. Comput. Control Syst. ICICCS 2018*, no. Iciccs, pp. 134–139, 2019, doi: 10.1109/ICCONS.2018.8662939.

[26] I. Inca, T. W. Widodo, and D. Lelono, ‘Klasifikasi Teh Hijau dan Teh Hitam Tambi-Pagilaran dengan Metode Principal Component Analysis (PCA) Menggunakan E-Nose’, *IJEIS (Indonesian J. Electron. Instrum. Syst.*, vol. 8, no. 1, pp. 61–72.

[27] Q. Wang, Q. Gao, X. Gao, and F. Nie, ‘Angle principal component analysis’, *IJCAI Int. Jt. Conf. Artif. Intell.*, vol. 0, pp. 2936–2942, 2017, doi: 10.24963/ijcai.2017/409.

[28] D. S. Putra, A. D. Wibawa, and M. H. Purnomo, ‘BERJALAN MENGGUNAKAN RANDOM FOREST’, vol. 1, no. 1, pp. 51–56, 2016.

[29] P. C. A. Mcsp, ‘SS symmetry Malware Classification Using Simhash Encoding and’, pp. 1–12, 2020.

[30] D. Han, Y. N. Rao, J. C. Principe, and K. Gugel, ‘implementation on DSP’, vol. 32, pp. 2159–2162.

[31] M. Ringnér, ‘What is principal component analysis ?’, vol. 26, no. 3, pp. 303–304, 2008.

[32] C. D. Morales-Molina, D. Santamaria-Guerrero, G. Sanchez-Perez, H. Perez-Meana, and A. Hernandez-Suarez, ‘Methodology for malware classification using a random forest classifier’, *2018 IEEE Int. Autumn Meet. Power, Electron. Comput. ROPEC 2018*, no. Ropec, pp. 1–6, 2019, doi: 10.1109/ROPEC.2018.8661441.

[33] M. Morchid, R. Dufour, P. M. Bousquet, G. Linarès, and J. M. Torres-Moreno, ‘Feature selection using Principal Component Analysis for massive retweet detection’, *Pattern Recognit. Lett.*, vol. 49, pp. 33–39, 2014, doi: 10.1016/j.patrec.2014.05.020.

[34] A. Primajaya *et al.*, ‘Random Forest Algorithm for Prediction of Precipitation’, vol. 1, no. 1, pp. 27–31, 2018.

[35] S. A. Roseline and S. Geetha, ‘Intelligent Malware Detection using Oblique Random Forest Paradigm’, *2018 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2018*, pp. 330–336, 2018, doi: 10.1109/ICACCI.2018.8554903.

[36] A. Luque, A. Carrasco, A. Mart\’\in, and A. de las Heras, ‘The impact of class imbalance in classification performance metrics based on the binary confusion matrix’, *Pattern Recognit.*, vol. 91, pp. 216–231, 2019.