KLASIFIKASI *MALWARE RANSOMWARE BERBASIS* TEKNIK SELEKSI FITUR DENGAN ALGORITMA *K-NEAREST NEIGHBOR*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

TATA SATRIA TIMOR PERDANA

09011381722118

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

KLASIFIKASI *MALWARE RANSOMWARE BERBASIS* TEKNIK SELEKSI FITUR DENGAN ALGORITMA *K-NEAREST NEIGHBOR*

TUGAS AKHIR

Diajukan untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

TATA SATRIA TIMOR PERDANA

09011381722118

Palembang, September 2021

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. H. Sukemi, M.T.	Ahmad Heryanto, S.Kom., M.T
NIP. 19661203200641001	NIP. 198701222015041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Jumat

Tanggal : 17 September 2021

Tim Penguji:

1. Ketua Sidang : Sarmayanta Sembiring, M.T.
2. Sekretaris Sidang : Aditya Putra Perdana P, S.Kom., M.T
3. Penguji Sidang : Deris Stiawan, M.T., PH.D.
4. Pembimbing : Ahmad Heryanto, S.Kom., M.T

Mengetahui, 4/10/21

Ketua Jurusan Sistem Komputer

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

NIP. 19661203200641001

iii

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Tata Satria Timor Perdana
NIM	: 09011381722118
Program Studi	: Sistem Komputer
Judul	: Klasifikasi *Malware Ransomware* Berbasis Teknik Seleksi Fitur Dengan Algoritma *K-Nearest Neighbor*

Hasil pengecekan *Software iThentivate/Turnitin* : 3%

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

Palembang, September 2021

Tata Satria Timor Perdana
09011381722118

iv

MOTTO DAN PERSEMBAHAN

MOTTO:

BUKAN SEBERAPA BESAR IPK MU TAPI SEBERAPA KUAT KAMU BERTAHAN DISETIAP SEMESTERNYA
APAPUN YANG SUDAH KAMU MULAI HARUS DI SELESAI KAN!

‘‘Karena sesungguhnya sesudah kesulitan itu ada kemudahan. Sesungguhnya sesudah kesulitan itu ada kemudahan” (QS. Al-Insyirah Ayat 5-6)

KU PERSEMBAHKAN UNTUK:

- ORANG TUA SAYA YANG 3T(TERCINTA, TERSAYANG DAN TERKEREN) DAN KELUARGA SAYA YANG SELALU MENDUKUNG DAN JUGA MEMBERIKAN SEMANAGAT KEPADA SAYA.
- TEMAN-TEMAN SEPERJUANGAN SISTEM KOMPUTER UNIVERSITAS SRIWIJAYA ANGKATAN 2017 YANG TIDAK AKAN TERLUPAKAN
- ALMAMATERKU UNIVERSITAS SRIWIJAYA

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan Proposal Tugas Akhir ini dengan judul "Klasifikasi *Malware Ransomware Berbasis* Teknik Seleksi Fitur Dengan Algoritma *K-Nearest Neighbor*".

Dalam laporan ini penulis menjelaskan mengenai penerapan metode Teknik Seleksi Fitur dan penerapan algoritma *K-Nearest Neighbor* untuk klasifikasi *malware* pada *Android*. Penulis berharap tulisan ini dapat bermanfaat bagi orang banyak, dan menjadi tambahan bahan bacaan bagi yang tertarik meneliti tentang *Android malware* serta penerapan Seleksi Fitur dan klasifikasi *malware* dan *benign*.

Pada penyusunan proposal tugas akhir ini, tidak terlepas dari bantuan, bimbingan serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan terima kasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan kemudahan, kesehatan, serta kesempatan dalam pelaksanaan pembuatan Tugas Akhir ini.
2. Ibu, Ayah serta Adik- adikku dan seluruh keluarga tercinta yang telah memberikan dukungan dan nasehat-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 Komputer Fakutas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, S.Kom., M.T selaku Pembimbing Tugas Akhir Penulis dan Bapak Sutarno, S.T., M.T. selaku Pembimbing Akademik di Jurusan Sistem Komputer. Terima kasih karena telah meluangkan waktunya untuk membimbing penulis, dalam menyelesaikan tugas akhir ini serta telah memberikan bimbingan dan nasehat selama perkuliahan.
6. Seluruh Dosen Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya.
7. Sahabat-Sahabatku tersayang, Rizky, Sumarno, Barzan, Ferdiyon, Nawawi, Rahmat, Steven, Devin, Dafi, Adam, Angga, Ari, Nuraini, Vanissa, Fidya, Vira, Tiara dan lain-lainnya.

8. Saudara-saudari seperjuangan untuk meraih kesuksesan Squad Duta Indo, Anak Waroeng Bawah, Teman-teman Asrama Brimob, dan alumni Sma Srijaya Negara beserta para guru.
9. Teman-teman seperjuangan angkatan 2017 dan anak-anak SK17 indralaya dan Palembang khususnya yang selalu membersamai selama perkuliahan ini.
10. Serta semua pihak yang telah membantu baik moril maupun materil yang tidak dapat disebutkan satu persatu dalam penyelesaian tugas akhir ini. Terima kasih banyak semuanya.

Penulis menyadari bahwa masih terdapat banyak kekurangan dalam penulisan Tugas Akhir ini, baik dari materi maupun teknik penyajiannya, mengingat kurangnya pengetahuan dan pengalaman penulis. Untuk itu, penulis mengharapkan adanya kritik dan saran yang membangun agar dapat memperbaiki kekurangan-kekungan tersebut kedepannya nanti.

Akhir kata dengan segala keterbatasan, penulis berharap semoga penulisan Tugas Akhir ini dapat menjadi tambahan wawasan dan ilmu pengetahuan bagi mahasiswa yang memerlukan khususnya mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran.

Palembang, Oktober 2021

Penulis

KLASIFIKASI *MALWARE RANSOMWARE BERBASIS* TEKNIK SELEKSI FITUR DENGAN *ALGORITMA K-NEAREST NEIGHBOR*

Tata Satria Timor Perdana (09011381722118)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : tatasatriatp@gmail.com

ABSTRAK

Malware adalah sebuah perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, ataupun server tanpa diketahui oleh pemiliknya, *Ransomware* merupakan jenis *malware* tertentu yang akan menuntut tebusan finansial dari korban dengan cara mengancam akan mempublikasikan, menghapus, atau juga menahan akses ke data pribadi yang penting. Pada penelitian ini akan melakukan klasifikasi terhadap *malware ransomware* berjenis *lockerpin* dengan berbasis teknik seleksi fitur dan menggunakan algoritma *K-Nearest Neighbor*. Teknik *Correlation* dan *Univariate* yang akan digunakan untuk tahap seleksi fitur yang kemudian akan di ambil fitur-fitur yang terbaik dan relevan. Dari hasil tersebut akan di lanjutkan dengan proses klasifikasi dengan menggunakan algoritma *K-Nearest Neighbor,* dengan melakukan 3 percobaan. Hasil yang didapatkan pada percobaan pertama *Correlation* 97,83% untuk *Univariate* 97,87%, percobaan kedua *correlation* 98,37% untuk *univariate* 98,80% dan percobaan ketiga *correlation* 98,80% untuk *univariate* 98,82%.

Kata kunci : *Malware, Ransomware, Lockerpin, K-Nearest Neighbor, Correlation, Univariate.*

CLASSIFICATION OF RANSOMWARE MALWARE BASED ON FEATURE SELECTION TECHNIQUES WITH K-NEAREST NEIGHBOR ALGORITHM

Tata Satria Timor Perdana (09011381722118)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : tatasatriatp@gmail.com

ABSTRACT

Malware is software that is created with the aim of entering and damaging computer systems, networks, or servers without the owner knowing, Ransomware is a certain type of malware that will demand a financial ransom from the victim by threatening to delete, or withhold access to important personal data. . In this study, we will classify the lockerpin type ransomware malware based on feature selection techniques and use the K-Nearest Neighbor algorithm. Correlation and Univariate techniques will be used for the feature selection stage which will then take the best and relevant features. From these results, it will be continued with the classification process using the K-Nearest Neighbor algorithm, by conducting 3 experiments. The results obtained in the first experiment Correlation 97.83% for Univariate 97.87%, the second experiment correlation 98.37% for univariate 98.80% and the third experiment correlation 98.80% for univariate 98.82%.

Keyword : Malware, Ransomware, Lockerpin, K-Nearest Neighbor, Correlation, Univariate.

DAFTAR ISI

HALAMAN

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Smartphone telah menjadi perangkat komunikasi dan komputasi inti saat ini. Dengan kemampuan yang lebih tinggi, perangkat ini tidak hanya digunakan untuk handset berorientasi suara sederhana komunikasi di masa lalu. Dengan kemampuan yang semakin meningkat mereka telah menjadi target untuk beberapa serangan *malware*. Itu pada tahun 2004, artikel pertama muncul di *smartphone malware*, yang melaporkan bahwa *smartphone* adalah target generasi berikutnya *malware*[1].

Malware adalah sebuah perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, ataupun server tanpa diketahui oleh pemiliknya. *Malware* merupakan salah satu ancaman *security* paling signifikan. *Malware* perangkat lunak dapat dikategorikan ke dalam kelas yang berbeda tergantung bagaimana mereka mencoba untuk merugikan atau berperilaku seperti *Trojan, Virus, Scareware, Worm, Ransomware* dan *Spyware*[2].

Ransomware merupakan jenis *malware* tertentu yang akan menuntut tebusan finansial dari korban dengan cara mengancam akan mempublikasikan, menghapus, atau juga menahan akses ke data pribadi yang penting. *Ransomware* ini sudah ada sejak akhir 1980-an, itu tidak mendapatkan banyak *popularitas* di kalangan penyerang sampai baru-baru ini, ketika beberapa teknologi yang memungkinkan seperti *Ransomware-asa-Service (RaaS)*, Internet, *kriptografi, Locker* dan yang sulit dilacak mata uang digital, telah muncul. Teknologi ini membuatnya mudah bahkan bagi penyerang pemula untuk mengembangkan dan menyebarkannya memiliki *ransomware* dan dapatkan bayaran tanpa takut ketahuan oleh pihak berwenang[3].

Hal ini merupakan sebuah bukti tindakan kejahatan pada aturan internet dilakukan oleh seseorang *hacker* dengan memanfaatkan *malware* sebagai medianya. *Google* juga sudah membuat *scanner security* berbasis *cloud rule* disebut *Bouncer* yang bertujuan untuk mendeteksi aplikasi berbahaya di *Play Store*. Akan tetapi masih ada saja aplikasi *yang* berisi *Malware* berhasil masuk ke dalam *Play Store* dan masih banyaknya pengguna *Android* yang mendownload aplikasi pada pihak ketiga, sehingga *smartphone* mereka masih

dapat terkena *Malware*. Oleh karena itu banyak dilakukan penelitan mengenai klasifikasi *malware* pada aplikasi *Android*[4].

Pada umumnya klasifikasi menggunakan semua fitur yang terdapat dalam data untuk membangun sebuah model, padahal tidak semua fitur tersebut relevan terhadap hasil klasifikasi. Jika hal tersebut terjadi pada data yang memiliki ukuran dan juga dimensi yang sangat besar, maka akan membuat kinerja algoritma menjadi tidak efektif dan efisien, misalkan saja waktu pemprosesan menjadi lebih lama akibat banyak fitur yang harus diproses. Jumlah banyaknya fitur tersebut dibutuhkan oleh sebuah sistem klasifikasi *malware* dengan teknik seleksi fitur untuk menghasilkan designation rule lebih efektif dan akurat[5].

Seleksi Fitur merupakan suatu proses untuk mengurangi dimensi atribut. Pengurangan dimensi tersebut dilakukan untuk mendapatkan atribut-atribut yang relevan dan tidak berlebihan sehingga dapat mempercepat proses klasifikasi dan dapat meningkatkan akurasi dari algoritme klasifikasi[6]. Metode seleksi fitur yang digunakan pada penelitian[7], Dalam proses pemilihan fitur dilakukan dengan menggunakan teknik diskriminatif yang berbeda. Pemilihan fitur yang dihasilkan juga dinilai dengan menggunakan empat teknik klasifikasi *biner* yang terkenal. Akurasi yang tinggi menunjukkan bahwa fitur yang diusulkan cukup diskriminatif untuk tujuan yang telah ditetapkan, mereka mendapatkan akurasi sebesar 96% dengan *K-Nerest Neighbor*.

Pada penelitian [8], mengusulkan sebuah pendekatan berbasis pembelajaran mesin yang efektif untuk *Android Malware* Deteksi menggunakan algoritma genetika evolusioner untuk pemilihan fitur diskriminatif. Hasil eksperimen memvalidasi itu Algoritma genetik memberikan bantuan subset fitur yang paling optimal pengurangan dimensi fitur menjadi kurang dari setengah aslinya set fitur. Akurasi klasifikasi lebih dari 94% adalah pemilihan fitur postingan yang dipertahankan untuk berbasis pembelajaran mesin pengklasifikasi, saat mengerjakan dimensi fitur yang jauh berkurang, dengan demikian, berdampak positif pada kompleksitas komputasi pengklasifikasi belajar.

Sedangkan pada penelitian [3], mengusulkan sebuah Redundansi baru Teknik *Coefficient Gradual Upweighting (RCGU)* yang membuat pengorbanan relevansi dan redundansi yang lebih baik selama pemilihan fitur, Teknik Gain Ratio digunakan untuk pemilihan fitur yang menunjukkan bahwa 1000 fitur merupakan angka optimal untuk proses deteksi. Mereka mendapatkan akurasi 95% dengan algoritma *K-Nerest Neighbor*.

Berdasarkan ulasan diatas, Penelitian[7] dalam prosesnya memakan waktu yang lama dan banyak data yang terlewatkan. Penelitian[8] mereka hanya menggunakan satu fitur yaitu subset fitur untuk mengurangi kompleksitas pelatihan pengklasifikasi. Penelitian[3] tersebut ada salah satu batasan dari Teknik RCGU yang diusulkan adalah kurangnya pertimbangan kondisional istilah redundansi saat menghitung signifikansi fitur. Untuk mengatasi kekurangan tersebut perlu dilakukan penelitian yang lebih baik yang tidak membutuhkan waktu lama dan memilih fitur yang baik dalam proses untuk klasifikasi *malware Android* agar dapat mengatasi masalah diatas.

Maka penelitian ini akan membahas mengenai klasifikasi *malware ransomware* berbasis teknik seleksi fitur dengan algoritma klasifikasi *K-Nearest Neighbor* dengan dua bentuk dataset normal dan *malware* yang akan diklasifikasi dengan dua seleksi fitur yaitu *correlation* dan *univariate* untuk mengurangi kompleksitas pelatihan pengklasifikasi dan mendapatkan tingkat akurasi yang tinggi.

1.2 Tujuan

Adapun tujuan yang ingin dicapai dari penelitian tugas akhir ini adalah:

1. Untuk mengimplementasikan fitur seleksi dalam klasifikasi *malware ransomware* dengan algoritma *K-Nearest Neighbor*
2. Melakukan analisis terhadap hasil klasifikasi Fitur seleksi dengan algoritma *K-Nearest Neighbor*

1.3 Manfaat

Adapun manfaat dari penelitian tugas akhir yang dilakukan, antara lain:

1. Dapat memperoleh tingkat akurasi dari proses fitur seleksi dalam klasifikasi *malware ransomware*.
2. Dapat mempelajari proses fitur seleksi dalam klasifikasi *malware ransomware*.

1.4 Rumusan Masalah

Berdasarkan dari latar belakang masalah yang ada, permasalahan yang dibahas pada penelitian ini yaitu:

1. Bagaimana menerapkan fitur seleksi yang digunakan untuk meningkatkan efektifitas dan efisiensi kinerja pada metode *K-Nearest Neighbor* dalam mengklasifikasi *malware ransomware*.

1.5 Batasan Masalah

Dari rumusan masalah dan latar belakang penelitian, maka berikut ini batasan masalah pada tugas akhir, antara lain :

1. Data yang digunakan dalam penelitian ini merupakan data *malware Android* baru yang disebut CICAndMal2017[9] yaitu *LockerPIN Ransomware*.
2. Mengklasifikasikan menggunakan fitur seleksi *Corelation* dan *Univariate* dengan algoritma *K-Nearest Neighbor*.

1.6 Metodologi Penelitian

Berikut adalah tahapan penelitian yang dilakukan untuk mencapai tujuan penelitian tugas akhir ini:

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 (Prosesing pengubahan data PCAP ke csv menggunakan CICFLOWMETER)
   Tahap ini membahas mengenai proses untuk mempersiapkan data yang akan digunakan.

3. Tahap Ketiga (Pengujian)
   Tahap ini merupakan tahap lanjutan dari proses tahap kedua yang telah dilakukan. Dengan melakukan pengujian berdasarkan fitur seleksi dan tidak memakai fitur seleksi dengan algoritma *K-Nerest Neighbor*.

4. Tahap Keempat (Analisa)
   Data yang diperoleh dari proses pengujian, kemudian dianalisis, 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.

1.7 Sistematika Penulisan

Untuk memudahkan dalam menyusun tugas akhir ini serta memperjelas isi dari setiap bab yang ada pada laporan ini, dibuatlah penulisan sistematika dari penelitian ini sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisi uraian latar belakang secara sistematis topik yang diambil.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang literatur yang relevan, kerangka teori dan kerangka berfikir.

BAB III METODOLOGI

Bab ini menjelaskan secara bertahap dan terperinci tentang langkah-langkah yang akan digunakan untuk mencari dan menganalisa tema dalam penulisan tugas akhir.

BAB IV PENGUJIAN DAN ANALISA

Bab ini menjelaskan tentang hasil dari pengujian yang telah dilakukan dan analisa terhadap hasil klasifikasi yang telah dibuat.

BAB IV KESIMPULAN

Bab ini berisi kesimpulan yang diperoleh oleh penulis serta merupakan jawaban dari setiap tujuan yang ingin dicapai pada bab I (Pendahuluan).

DAFTAR PUSTAKA

[1] V. P. D and V. P, "Detecting android malware using an improved filter based technique in embedded software," *Microprocess. Microsyst.*, vol. 76, p. 103115, 2020.

[2] I. Shhadat, B. Bataineh, A. Hayajneh, and Z. A. Al-Sharif, "The Use of Machine Learning Techniques to Advance the Detection and Classification of Unknown Malware," *Procedia Comput. Sci.*, vol. 170, no. 2019, pp. 917–922, 2020.

[3] B. A. S. Al-rimy *et al.*, "Redundancy Coefficient Gradual Up-weighting-based Mutual Information Feature Selection technique for Crypto-ransomware early detection," *Futur. Gener. Comput. Syst.*, vol. 115, pp. 641–658, 2021.

[4] P. Kaur and S. Sharma, "Spyware detection in android using hybridization of description analysis, permission mapping and interface analysis," *Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 794–803, 2015.

[5] A. Pektaş and T. Acarman, "Classification of malware families based on runtime behaviors," *J. Inf. Secur. Appl.*, vol. 37, pp. 91–100, 2017.

[6] L. Cai, Y. Li, and Z. Xiong, "JOWMDroid: Android malware detection based on feature weighting with joint optimization of weight-mapping and classifier parameters," *Comput. Secur.*, vol. 100, p. 102086, 2021.

[7] L. F. Martín Liras, A. R. de Soto, and M. A. Prada, "Feature analysis for data-driven APT-related malware discrimination," *Comput. Secur.*, vol. 104, 2021.

[8] A. Fatima, R. Maurya, M. K. Dutta, R. Burget, and J. Masek, "Android malware detection using genetic algorithm based optimized feature selection and machine learning," *2019 42nd Int. Conf. Telecommun. Signal Process. TSP 2019*, pp. 220–223, 2019.

[9] 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.

[10] S. Saeed, N. Z. Jhanjhi, M. Naqvi, M. Humayun, and S. Ahmed, "Ransomware: A framework for security challenges in internet of things," *2020 2nd Int. Conf. Comput. Inf. Sci. ICCIS 2020*, 2020.

[11] M. Alazab, "Automated malware detection in mobile app stores based on robust feature generation," *Electron.*, vol. 9, no. 3, 2020.

[12] G. A. Sandag, J. Leopold, and V. F. Ong, "Klasifikasi Malicious Websites Menggunakan Algoritma K-NN Berdasarkan Application Layers dan Network Characteristics," *CogITo Smart J.*, vol. 4, no. 1, p. 37, 2018.

[13] J. Maestre Vidal, A. L. Sandoval Orozco, and L. J. García Villalba, “Alert correlation framework for malware detection by anomaly-based packet payload analysis,” *J. Netw. Comput. Appl.*, vol. 97, pp. 11–22, 2017.

[14] F. Shang, Y. Li, X. Deng, and D. He, “Android malware detection method based on naive bayes and permission correlation algorithm,” *Cluster Comput.*, vol. 21, no. 1, pp. 955–966, 2017.

[15] A. Rahmansyah, O. Dewi, P. Andini, T. Hastuti, P. Ningrum, and M. E. Suryana, “Membandingkan Pengaruh Feature Selection Terhadap Algoritma Naïve Bayes dan Support Vector Machine,” *Semin. Nas. Apl. Teknol. Inf.*, pp. 1–7, 2018.

[16] A. Bommert, X. Sun, B. Bischl, J. Rahnenführer, and M. Lang, “Benchmark for filter methods for feature selection in high-dimensional classification data,” *Comput. Stat. Data Anal.*, vol. 143, p. 106839, 2020.

[17] M. B. B. De Robles, J. M. Samaniego, and J. A. C. Hermocilla, “Characterization and Classification of Malware Traffic over the Tor Network,” no. January, pp. 78–87, 2020.

[18] W. Cherif, “Optimization of K-NN algorithm by clustering and reliability coefficients: Application to breast-cancer diagnosis,” *Procedia Comput. Sci.*, vol. 127, pp. 293–299, 2018.

[19] M. Nanja and P. Purwanto, “Metode K-Nearest Neighbor Berbasis Forward Selection Untuk Prediksi Harga Komoditi Lada,” *Pseudocode*, vol. 2, no. 1, pp. 53–64, 2015.

[20] G. Baldini and D. Geneiatakis, “A performance evaluation on distance measures in KNN for mobile malware detection,” *2019 6th Int. Conf. Control. Decis. Inf. Technol. CoDIT 2019*, pp. 193–198, 2019.

[21] Z. Zhai, H. Jiang, L. Lu, and Y. Liu, “Adaptive truncation coding for computed tomography images,” *Proc. 2014 Int. Symp. Inf. Technol. ISIT 2014*, vol. 02, no. 1, pp. 115–118, 2015.

[22] R. A. Arnomo, W. L. Y. Saptomo, and P. Harsadi, “Implementasi Algoritma K-Nearest Neighbor Untuk Identifikasi Kualitas Air (Studi Kasus : Pdam Kota Surakarta),” *J. Teknol. Inf. dan Komun.*, vol. 6, no. 1, 2018.

[23] A. Y. Saputra and Y. Primadasa, “Penerapan Teknik Klasifikasi Untuk Prediksi Kelulusan Mahasiswa Menggunakan Algoritma K-Nearest Neighbor,” *Techno.Com*, vol. 17, no. 4, pp. 395–403, 2018.

[24] X. Zhou, J. Pang, and G. Liang, “Image classification for malware detection using extremely randomized trees,” *Proc. Int. Conf. Anti-Counterfeiting, Secur. Identification, ASID*, vol. 2017-Octob, no. 61472447, pp. 54–59, 2018.

[25] M. Noorani, S. Mancoridis, and S. Weber, “On the Detection of Malware on Virtual Assistants Based on Behavioral Anomalies.”