KLASIFIKASI MALWARE TROJAN BANKING PADA ANDROID MENGGUNAKAN METODE ALGORITMA SUPPORT VECTOR MACHINE

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

Ni Komang Tri Lestari

09011381722127

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

KLASIFIKASI MALWARE TROJAN BANKING PADA ANDROID MENGGUNAKAN METODE ALGORITMA SUPPORT VECTOR MACHINE

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :
Ni Komang Tri Lestari
09011381722127

Palembang, November 2021

Mengetahui,

Pembimbing I Tugas Akhir	Pembimbing II Tugas Akhir
Ahmad Heryanto, M.T.	Ahmad Fali Oklilas, M.T.
NIP. 198701222015041002	NIP. 197210151999031001

Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

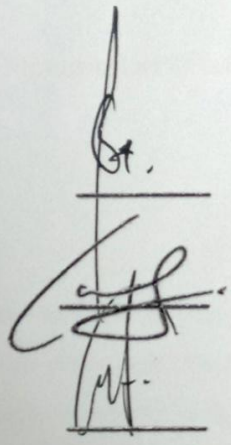
Telah diuji dan lulus pada:

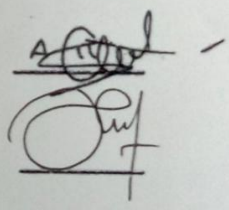
Hari : Rabu

Tanggal : 3 November 2021

Tim Penguji:

1. **Ketua : Sutarno, M.T.**
2. **Sekretaris : Iman Saladin B Azhar, M.MSI.**
3. **Penguji : Ahmad Zarkasi, M.T.**
4. **Pembimbing I : Ahmad Heryanto, M.T.**
5. **Pembimbing II : Ahmad Fali Oklilas, M.T.**





Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Ni Komang Tri Lestari
NIM : 09011381722127
Judul : Klasifikasi Malware Trojan Banking pada Android Menggunakan Metode Algoritma Support Vector Machine

Hasil pengecekan Plagiat/Turnitin : 4%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil plagiat atau penjiplakan. 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 dari pihak manapun.

Palembang, November 2021

Yang menyatakan,

Ni Komang Tri Lestari

NIM : 09011381722127

KATA PENGANTAR

Om Swastyastu

Astungkare atas asung kerta wara nugraha ida Sang Hyang Widhi Wasa saya dapat menyelesaikan penyusunan Tugas Akhir ini dengan judul ‘‘*Klasifikasi Malware Trojan Banking* Pada *Android* Menggunakan Metode *Algoritma Support Vector Machine*’’ dengan baik.

Dalam Tugas Akhir ini penulis menjelaskan mengenai Klasifikasi *malware* jenis *Trojan Banking* pada *android* dengan menggunakan Metode *Algoritma Support Vector Machine* 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 dan terimakasih kepada yang terhormat :

1. Ida Sang Hyang Widhi Wasa yang telah memberikan kemudahan, kesehatan, serta kesempatan dalam melaksanaan pembuatan Tugas Akhir ini.
2. Kedua orang tua, saudara, dan Keluarga Besar yang selalu mendoakan dan selalu memberikan motivasi, semangat dukungannya.
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 dan Dosen Pembimbing Akademik di Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, M.T. selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Ahmad Fali Oklilas, M.T. selaku dosen pembimbing II Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

7. Seluruh Dosen, Staff dan karyawan Fakultas Ilmu Komputer Universitas Sriwijaya
8. Seseorang yang istimewa yang selalu mengingatkan, dan memberikan semangat serta support.
9. Teman-teman seperjuangan Sistem Komputer Angkatan 2017 Bukit yang selalu memberi dukungan.
10. Teman-teman seperjuangan Kedal Squad, yang selalu memberikan dukungan.
11. Dan semua kerabat yang tidak dapat saya sebutkan satu persatu.

Tiada lain harapan saya semoga ida Sang Hyang Widhi Wasa membalas segala niat baik kepada semua pihak yang saya sebutkan diatas. Saya menyadari bahwa 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 bermanfaat bagi semuanya. Sebelum dan sesudahnya penulis mengucapkan terimakasih.

Om shanti shanti shanti om

Palembang, November 2021

Ni Komang Tri Lestari

KLASIFIKASI MALWARE TROJAN BANKING PADA ANDROID MENGGUNAKAN METODE ALGORITMA SUPPORT VECTOR MACHINE

Ni Komang Tri Lestari (09011381722127)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
E-mail : nikomangtrilestari@gmail.com

Abstrak

Malware sangat berbahaya karna dapat merugikan banyak orang, salah satu malware yang sangat berbahaya ini adalah Malware Trojan Banking yang dirancang untuk mencuri uang langsung dari rekening bank para pengguna PC maupun mobile. Kehidupan kita yang semakin mobile, aplikasi perbankan dengan cepat menjadi metode yang tepat untuk mengelola keuangan. Pembuat malware yang termotivasi oleh keuntungan finansial ini dengan cepat mengadaptasi dan mengggunakan alat dan teknik mereka untuk mendapatkan keuntungan. Metode *Algoritma Support Vector Machine* dapat dilakukan untuk melakukan klasifikasi Malware Trojan Banking pada Android, dimana klasifikasi malware Trojan Banking pada Android ini berfokus pada *Malware Trojan Banking* dan *Benign*. Dataset yang digunakan bersumber dari internet tepatnya di CICMaldroid 2020, hasil akurasi dengan menerapkan *Algoritma Support Vector Machine* ini adalah 95.268%.

Kata kunci **:** Klasifikasi**,** Trojan Banking, Malware, Android, Support Vector Machine.

CLASIFICATION MALWARE TROJAN BANKING ON ANDROID USING SUPPORT VECTOR MACHINE ALGORITHM METHOD

Ni Komang Tri Lestari (09011381722127)
Departement of Computer Engineering, Faculty of Computer Science, Sriwijaya University
E-mail : nikomangtrilestari@gmail.com

Abstract

Malware is very dangerous because it can harm many people, one of these very dangerous malware is the Malware Trojan Banking which is designed to steal money directly from the bank accounts of PC and mobile users. In our increasingly mobile life, banking applications are quickly becoming the right method for managing finances. These financially motivated malware authors quickly adapt and use their tools and techniques to their advantage. The Support Vector Machine Algorithm method can be used to classify Malware Trojan Banking on Android, where the classification of Malware Trojan Banking on Android focuses on Malware Trojan Banking and Benign. The dataset used is sourced from the internet, precisely at CICMaldroid 2020, the accuracy result by applying the Support Vector Machine Algorithm is 95.268%.

Keywords **:** Clasification**,** Trojan Banking, Malware, Android, Support Vector Machine.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1. Latar Belakang

Android adalah salah satu alat untuk berproses yang berjenis linux, sangat membantu pengguna untuk melakukan aktivitas contohnya seperti melakukan komunikasi, shopping online, dan lain sebagainya. Keunggulan sistem operasi android dibanding dengan sistem operasi smartphone lainnya adalah android bersifat open source code sehingga memudahkan para pengembang untuk membuat dan memodifikasi aplikasi atau filtur-filtur yang belum terdapat pada sistem operasi android sesuai dengan kebutuhan. Seiring dengan perkembangan teknologi, tidak bisa dihindari berkembangnya file yang tidak baik. File-file yang tidak baik adalah malware[2].

Malware adalah perangkat yang memiliki tujuan untuk memperusak perangkat lunak komputer yang ada dalam berbagai bentuk seperti script, code, active, content, dan perangkat lunak[1]. Secara eksplisit, malware merupakan perangkat lunak yang dibuat untuk melakukan aktifitas yang dapat merusak aplikasi lainnya seperti Trojan, Virus, Spyware dan Exploit. Online perbankan berfungsi untuk melakukan proses seperti pengambilan uang dan penambahan uang menggunakan aplikasi e-banking, e-commerce, dan elektronik pembayaran lainnya tanpa mengeluarkan tenaga dan usaha lagi untuk melakukan transaksi ke bank[3]. Kehidupan kita yang semakin maju atau saya katakana mobile, aplikasi perbankan dengan cepat menjadi metode yang tepat untuk mengelola keuangan. Pembuat malware yang termotivasi oleh keuntungan finansial dengan cepat mengadaptasi dan mengggunakan alat dan teknik mereka untuk mendapatkan keuntungan dari kemajuan ini. Sehingga dapat mengakibatkan malware mobile banking menargetkan plaffrom android telah menjadi ancaman yang sangat nyata dan kuat, namun sering diremehkan oleh masyarakat[10]

Dalam penelitian melakukan klasifikasi jenis malware pada *Android* dan juga mengetahui seberapa besar akurasi yang di dapat, banyak metode yang telah diterapkan pada penelitian sebelumnya. diantaranya adalah metode *Random Forest*, dan *K-nears Nighbor (KNN)* akan tetapi dari penelitian yang menggunakan metode *Random Forest*, dan *K-nears Nighbor (KNN)* akurasinya sangat kecil. Akurasi yang didapat adalah 63.49% [5].

Dengan mengacu pada penelitian terdahulu untuk memperoleh performasi yang akurat, maka penulis akan menerapkan Algoritma *Support Vector Machine* untuk mengkasifikasikan Malware Android yang berjenis Trojan Banking. Dimana klasifikasi ini berpusat pada malware banking dan benign dengan menggunakan *dataset CICMalDroid 2020* diambil dari internet tepatnya di UNB (university of new Brunswick). Metode support vector machine (*SVM)* berfungsi untuk memisahkan 2 set atau lebih dari 2 kelas yang berbeda.

Dari uraian diatas maka dapat disimpulkan bahwa pembahasan ini adalah tentang bagaimana pentingnya melakukan klasifikasi malware Trojan banking pada android agar mendapatkan jumlah akurasi yang maksimal. Sehingga tugas akhir ini berjudul "*Klasifikasi Malware Trojan Banking pada Android menggunakan metode algoritma SVM (Support Vector Machine)*".

1.2. Rumusan Masalah

Dari penjelasan yang telah diuraikan pada bagian latar belakang diatas, maka dapat diambil rumusan masalah yaitu "Bagaimana menerapkan algoritma *Support Vector Machine* dalam melakukan klasifikasi *malware* jenis *Trojan Banking* pada *Android*?".

1.3. Batasan Masalah

Terdapat 3 Batasan masalah yang diterapkan pada penelitian ini diantaranya adalah:

1. Klasifikasi *malware* hanya jenis *Trojan Banking*

2. Algortima yang digunakan dalam Klasifikasi *malware* jenis *Trojan Banking* hanya menggunakan algortima *Support Vector Machine*.
3. Klasifikasi menggunakan *dataset CICMalDroid2020* diambil dari internet tepatnya di UNB (university of new Brunswick).

1.4. Tujuan dan Manfaat

1.4.1. Tujuan

1. Tujuannya adalah untuk klasifikasi malware jenis *Trojan Banking* pada *Android* menggunakan Metode *Support Vector Machine*.
2. Tujuannya adalah untuk mengetahui informasi mengenai performa dari metode support vector machine.

1.4.2. Manfaat

1. Untuk mengetahui bagaimana cara menerapkan algoritma *Support Vector Machine* dalam melakukan klasifikasi terhadap *Trojan Banking* pada *Android*.

2. Untuk memberikan informasi mengenai performace metode *Support Vector Machine.*

1.5. Metodelogi Penelitian

Metodologi yang akan digunakan dalam penelitian ini diwakilkan dengan beberapa tahap sebagai berikut:

1. Tahapan Perumusan masalah

   Tahap pertama adalah tahap perumusan masalah yaitu penentuan pokok permasalahan mengenai klasifikasi Malware android.

2. Tahapan Pustaka

   Tahap kedua adalah tahap literature yaitu penulis mengumpulkan referensi yang diambil dari paper dan jurnal yang berkaitan dengan metode Support vector machine atau bisa juga dengan jenis metode lain sebagai referensi.

3. Tahapan Rancang Sistem

   Tahap ketiga yakni tahap perancangan sistem, berdasarkan tahap pertama dan tahap kedua yang digunakan.

4. Tahapaan Pengujian

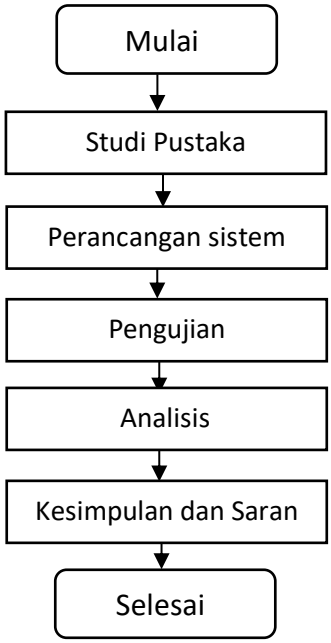
   Tahap keempat adalah tahap pengujian dimana pada tahap ini penulis menguji dengan menggunakan algoritma dan kodingan yang telah dibuat pada python untuk mendapatkan hasil maksimal dalam melakukan klasifikasi malware trojan banking.

5. Tahapan Analisia

   Tahap kelima adalah tahap Analisa dimana pada tahap ini penulis memberi analisa hasil yang didapat pada saat melakukan klasifikasi malware Trojan Banking.

6. Tahapan Kesimpulan dan saran

   Tahap keenam adalah tahap kesimpulan dan saran, pada tahap ini penulis memberikan kesimpulan akhir dari hasil penilitian yang telah diselesaikan dan memberikan saran untuk penelitian selanjutnya. Berikut dibawah ini gambar tampilan proses penelitian :



Gambar 1.1 Tampilan Proses Penelitian

1.6. Sistematika Penulisan

Adapun sistematika penulisan yang digunakan dalam melakukan penelitian tugas akhir ini adalah sebagai berikut:

BAB I BAB I PENDAHULUAN

Pada Bab pertama menjelaskan tentang judul yang didalam judul itu terdapat latar belakang, perumusan masalah, batasan masalah, tujuan serta penataan pada penulisan skripsi.

BAB II TIJAUAN PUSTAKA

Bab kedua ini menjelaskan dasar teori yang menunjang pembahasan dari penelitian ini. Dasar teori ini berisi tentang klasifikasi, malware, Trojan banking, android dan metode yang digunakan.

BAB III METODOLOGI PENELITIAN

Bab 3 ini menjelaskan tentang Struktur proses yang akan dijalankan pengambilan dataset, dan juga perancangan sistem.

BAB IV HASIL DAN ANALISIS

Pada Bab keempat ini menjelaskan hasil yang diperoleh, setelah mendapatkan hasil penulis manganalisa hasil yang didapat..

BAB V KESIMPULAN

Selanjutnya adalah bab V kesimpulan, dimana pada bab ini penulis memberikan kesimpulan berdasarkan poin utama (inti dari penelitian) yang telah diperoleh.

Daftar Pustaka

[1] 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.

[2] H. Saputra, S. Basuki, and M. Faiqurahman, "Implementasi teknik seleksi fitur pada klasifikasi malware Android menggunakan support vector machine (SVM)," *Repositor*, vol. 1, no. 1, p. 1, 2019, doi: 10.22219/repositor.v1i1.1.

[3] J. S. Komputer, F. I. Komputer, and U. Sriwijaya, "SISTEM PENCEGAHAN SERANGAN MALWARE BANKING TROJAN DENGAN METODE RANDOM," 2020.

[4] S. Mahdavifar, A. Fitriah, A. Kadir, R. Fatemi, D. Alhadidi, and A. A. Ghorbani, "Dynamic Android Malware Category Classification using Semi-Supervised Deep Learning," pp. 515–522, 2020, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00094.

[5] V. Rahmayanti *et al.*, "Klasifikasi Malware Family Menggunakan Metode K-Nearest Neighbor," pp. 319–323, 2020.

[6] I. Fakultas, U. P. Harapan, D. E. Ratnawati, and A. W. Widodo, "Klasifikasi Penyakit Gigi Dan Mulut Menggunakan Metode Support Vector Klasifikasi Penyakit Gigi Dan Mulut Menggunakan Metode Support Vector Machine," no. January, 2018.

[7] E. S. Lamdompak Sistem Komputer and F. Ilmu Komputer, “Klasifikasi Malware Trojan Ransomware Dengan Algoritma Support Vector Machine (SVM),” vol. 2, no. 1, pp. 122–127, 2016.

[8] M. M. Diani, “Tugas akhir – ks 141501,” p. 158, 2017.

[9] T. Singh, F. Di Troia, V. A. Corrado, T. H. Austin, and M. Stamp, “Support vector machines and malware detection,” *J. Comput. Virol. Hacking Tech.*, vol. 12, no. 4, pp. 203–212, 2016, doi: 10.1007/s11416-015-0252-0.

[10] L. Štefanko, “Android Banking Malware : Sophisticated Trojans Vs . Fake Banking Apps,” 2019.

[11] S. Huang, C. A. I. Nianguang, P. Penzuti Pacheco, S. Narandes, Y. Wang, and X. U. Wayne, “Applications of support vector machine (SVM) learning in cancer genomics,” *Cancer Genomics and Proteomics*, vol. 15, no. 1, pp. 41–51, 2018, doi: 10.21873/cgp.20063.

[12] B. S. Khehra and A. P. S. Pharwaha, “Classification of clustered microcalcifications using MLFFBP-ANN and SVM,” *Egypt. Informatics J.*, vol. 17, no. 1, pp. 11–20, 2016, doi: 10.1016/j.eij.2015.08.001.

[13] D. C. Soraya, “Klasifikasi android malware menggunakan algoritma principal component analysis (pca) dan random forest,” 2020.