Klasifikasi *Malware Banking* Pada Android Dengan Metode *Support Vector Machine*

TUGAS AKHIR

Oleh:

OCTAFIAN
09011181621002

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

Klasifikasi *Malware Banking* Pada Android Dengan Metode *Support Vector Machine*

TUGAS AKHIR

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

Oleh:

OCTAFIAN
09011181621002

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN

KLASIFIKASI MALWARE BANKING PADA ANDROID DENGAN METODE SUPPORT VECTOR MACHINE

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

OCTAFIAN

09011181621002

Inderalaya, Juni 2021

Pembimbing I Tugas Akhir	Pembimbing II Tugas Akhir
Deris Stiawan,M.T.,Ph.D	**Ahmad Heryanto,S.Kom.,M.T**
NIP.197806172006041002	**NIP.198701222015041002**

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr.Ir.Sukemi, MT
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis

Tanggal : 01 April 2021

Tim Penguji:

1. **Ketua Sidang** : **Sarmayanta Sembiring, S.SI., M.T.** (.....)
2. **Sekretaris Sidang** : **Rendyansyah, S.Kom., M.T.** (.....)
3. **Penguji SIdang** : **Huda Ubaya, S.T., M.T.** (.....)

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, MT
NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : **OCTAFIAN**

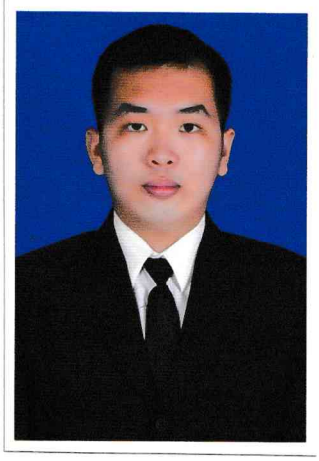
NIM : **09011181621002**

Judul : **Klasifikasi Malware Banking Pada Android Dengan Algoritma *Support Vector Machine***

Hasil Pengecekan Software iThenticate/Turnitin : 14 %

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil pejiplakan / *plagiat*. Apabila ditemukan unsur penjiplakan / *plagiat* dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, Pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



Palembang, Maret 2021

OCTAFIAN

NIM. 09011181621002

HALAMAN PERSEMBAHAN

Kutipan:

"Jangan berlebihan menilai apa yang kamu terima, apalagi iri dengan milik orang lain. Dia yang iri dengan milik orang lain sulit mendapatkan kedamaian batin."
(Sang Buddha)

"Satu-satunya kegagalan sesungguhnya dalam hidup adalah tidak menjadi yang terbaik yang kita tahu."
(Sang Buddha)

"Tidak ada yang menyelamatkan kita kecuali diri kita sendiri. Tidak ada yang bisa dan tidak ada yang mampu. Diri kita sendiri harus mampu melangkah pada jalan yang kita tuju."
(Sang Buddha)

"Jangan memikirkan masa lalu, jangan memimpikan masa depan, konsentrasikan pikiran pada saat sekarang.
(Sang Buddha)

"Jika masalah dapat diatasi, jika satu situasi dapat kamu hadapi dengan baik, maka kamu tidak perlu cemas. Jika masalah tidak dapat kamu perbaiki dan kamu menghadapi situasi yang kamu sendri tidak dapat melakukan apa apa, maka merasa cemas tidak akan menyelesaikan masalah."
(Dalai Lama)

Tugas Akhir ini kupesembahkan untuk:

- ***Sang Buddha.***
- ***Kedua orang tua, Saudaraku dan Keluarga besar.***
- ***Sahabat – sahabatku yang selalu ada bersamaku disaat senang maupun susah.***
- ***Rekan – rekan seperjuangan di Sistem Komputer 2016.***
- ***Jurusanku, Sistem Komputer.***
- ***Almamaterku, Universitas Sriwijaya.***

KATA PENGANTAR

Puji syukur atas kehadirat Tuhan Yang Maha Esa, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan Tugas Akhir ini dengan judul **"**Klasfikasi Malware Banking Pada Android Dengan Metode *Support Vector Machine***"**.

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 tugas akhir 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 Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Tuhan Yang Maha Esa. dan mengucapkan terima kasih kepada yang terhormat :

1. Orang Tua serta keluarga penulis tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama mengikuti dan melaksanakan perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya hingga dapat menyelesaikan Proposal Tugas Akhir ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Ibu Prof. Dr. Ir. Siti Nurmaini, M.T. selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph.D selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

6. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing II Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Mbak Nurul Afifah, S.Kom, M.Kom yang telah sangat membantu saya dalam penulisan proposal tugas akhir ini.
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Adik tingkatku Abdi Bimantara yang telah banyak membantu dalam pengerjaan tugas akhir ini.
10. Sahabatku Ahmad Aji Guntur Saputra yang telah memberikan semangat dalam penulisan proposal tugas akhir ini.
11. Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
12. Almamater.

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 Tugas Akhir ini dapat bermanfaat dan berguna bagi pembaca.

Palembang, Juni 2021
Penulis

OCTAFIAN

KLASIFIKASI *MALWARE BANKING* PADA ANDROID DENGAN METODE *SUPPORT VECTOR MACHINE*

OCTAFIAN (09011181621002)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : octafian456@gmail.com

ABSTRAK

Klasifikasi *malware* adalah cara untuk mengenali jenis data yang digolongkan sebagai malware atau normal file. *Banking Malware* merupakan jenis trojan yang bertujuan untuk menipu nasabah bank dan lembaga keuangan, sehingga memungkinkan korban untuk mentransfer dana dari rekening korban ke rekening penyerang. Tujuan dari penelitian ini adalah untuk mendapatkan tingkat akurasi terbaik dalam klasifikasi *Banking Malware* menggunakan metode *support vector machine* dengan menggunakan dataset yang berasal dari *Universitas of New Brunswick* yaitu CICMALDROID2020. Fitur ekstraksi pada penelitian menggunakan tools *CICFlowMeters* untuk mengubah file menjadi siap olah. Pada Penelitian ini juga menggunakan *feature selection extra-tree classifier* yang bertujuan untuk memilih fitur terbaik. Hasil klasifikasi menggunakan metode *support vector machine* menunjukkan hasil yang cukup baik yaitu nilai akurasi sebesar 87% yang menandakan keakuratan dalam pengklasifikasian serangan malware banking pada penelitian ini.

Kata Kunci : Klasifikasi , *Banking Malware* , *CICFlowMeters*, *Extra tree Classifier*, *Support Vector Machine*

Mengetahui

Pembimbing I	**Pembimbing II**
Deris Stiawan, Ph.D.	**Ahmad Heryanto,S.Kom.,M.T**
NIP. 197806172006041002	**NIP.198701222015041002**

Ketua Jurusan Sistem Komputer

2/4/22

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

NIP. 196612032006041001

CLASSIFICATION OF MALWARE BANKING ON ANDROID WITH SUPPORT VECTOR MACHINE METHOD

OCTAFIAN (09011181621002)

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

Email : octafian456@gmail.com

ABSTRACT

Malware classification is a way to recognize types of data that are classified as malware or normal files. Banking Malware is a type of trojan that aims to deceive bank customers and financial institutions, allowing victims to transfer funds from the victim's account to the attacker's account. The purpose of this study is to obtain the best level of accuracy in the classification of Banking Malware using a support vector machine method using a dataset from the University of New Brunswick, namely the CICMALDROID2020. The extraction feature in the study uses the CICFlowMeters tool to convert files into ready-to-process files. This research also uses a feature selection extra-tree classifier which aims to select the best features. The results of the classification using the support vector machine method show fairly good results, namely an accuracy value of 87% which indicates the accuracy in the classification of banking malware attacks in this study.

Keywords *: Classification, Banking Malware , CICFlowMeters, Extra tree Classifier, Support Vector Machine*

Mengetahui

Pembimbing I	**Pembimbing II**
Deris Stiawan, Ph.D.	**Ahmad Heryanto,S.Kom.,M.T**
NIP. 197806172006041002	**NIP.198701222015041002**

Ketua Jurusan Sistem Komputer

2/07/21

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

NIP. 196612032006041001

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Banking Malware merupakan jenis trojan yang bertujuan untuk menipu nasabah bank dan lembaga keuangan, sehingga memungkinkan korban untuk mentransfer dana dari rekening korban ke rekening penyerang. *Banking Malware* biasanya didistribusikan melalui email phishing atau unduhan *Drive-by* [1]. Saat ini jumlah *Banking malware* mengalami peningkatan yang sangat pesat. Terdapat 98,5% *Banking malware* yang telah menargetkan *Android*. Oleh sebab itu membutuhkan proses seleksi yang tepat untuk menganalisis pemilihan klasifikasi serangan *Banking Malware* yang telah menargetkan *android* [2].

SVM adalah metode yang berfungsi untuk menganalisis data yang digunakan untuk klasifikasi dan analisis regresi. Salah satu ciri dari metode SVM adalah mencari garis pemisah (*hyperplane*) terbaik sehingga menghasilkan ukuran margin yang maksimal dari dua kelas tersebut [3]. Sebelum melakukan klasifikasi pada dataset *malware*, terlebih dahulu melakukan proses fitur seleksi untuk menghasilkan hasil klasifikasi yang baik. Proses fitur seleksi akan dilakukan menggunakan *Extra-tree classifier.*

Extra-tree classifier merupakan jenis teknik metode pembelajaran yang menggabungkan hasil dari beberapa pohon keputusan untuk mendapatkan hasil klasifikasi yang terbaik. *Extra-tree classifier* ini bertujuan untuk memberikan ranking pada fitur yang paling terbaik untuk diklasifikasikan menggunakan metode *Support Vector Machine*. Pada penelitian [4], membahas tentang deteksi android malware dengan menggunakan algoritma *Extra-Tress Classifier*. Data dalam penelitian ini berasal dari website *Universitas of New Brunswick* yang bernama CICAndMal2017. Data penelitian tersebut masih berupa pcap yang dimana harus menggunakan *CICFlowmeter* untuk mengubahnya menjadi format CSV.

Pada Penelitian [5], membahas klasifikasi *android malware* dengan membandingkan lima metode yaitu SVM, Naïve Baiyes, K-NN, Decesion Tree dan Logistic Regression. Dalam penelitian ini menunjukan tingkat akurasi setiap

metode yang dipakai untuk mengklasfikasi malware pada *android*. Hasilnya metode SVM memiliki akurasi 94,31% yang lebih tinggi dari lima metode tersebut.

Pada penelitian [6], membahas mengenai klasifikasi *malware* pada android menggunakan metode *support vector machine*. Dalam Penelitian ini menguji 400 aplikasi android pada dataset drebin. Penelitian ini menguji kumpulan aplikasi android pada dataset drebin. Hasil akurasi pada penelitian ini mencapai 81%. Berdasarkan ulasan diatas, penulis akan melakukan implementasi sistem klasifikasi *banking malware* menggunakan metode *support vector machine.*

1.2 Batasan dan Perumusan Masalah

Adapun batasan dan perumusan masalah dalam penulisan Proposal Tugas Akhir ini adalah sebagai berikut:

1.2.1 Batasan Masalah

Berikut adalah batasan masalah dalam penulisan Proposal Tugas Akhir ini:

1. Analisa *malware banking* dilakukan secara *statis.*
2. *Feature selection* yang digunakan adalah *Extra-Tress Classifier*
3. Metode yang digunakan adalah *Support Vector Machine*.
4. Dataset digunakan pada penelitian ini berasal dari *Universitas of New Brunswick* yaitu CICMALDROID2020.
5. Dalam penelitian ini tidak membahas bagaimana cara pencegahan *Banking Malware.*

1.2.2 Perumusan Masalah

Berikut adalah rumusan masalah dalam penulisan Proposal Tugas Akhir ini:

1. Bagaimana cara menerapkan algoritma *feature selection Extra-Tress Classifier* pada proses klasifikasi *malware banking*?
2. Bagaimana cara mengklasifikasikan *malware* pada android dengan menggunakan metode *Support Vector Machine*?

3. Bagaimana cara menvalidasi hasil dari proses klasifikasi metode *Support Vector Machine*?

1.3 Tujuan

Adapun tujuan dari penulisan Tugas Akhir ini adalah sebagai berikut :

1. Menerapkan algoritma *feature selection Extra-Tree Classifier* untuk meningkatkan hasil klasifikasi.
2. Mengklasifikasi data *malware banking android* dengan menggunakan metode *Support Vector Machine*.
3. Menvalidasi hasil dari proses klasifikasi metode *Support Vector Machine*.

1.4 Manfaat

Adapun manfaat dari penulisan Tugas Akhir
ini adalah sebagai berikut :

1. Mengetahui fungsi *feature selection Extra-Tree Classifier* untuk mendapatkan hasil akurasi yang terbaik.
2. Dapat mengklasifikasi *malware banking android* dengan menggunakan metode *Support Vector Machine*.
3. Dapat menvalidasi hasil dari proses klasifikasi metode *Support Vector Machine*.

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini akan melewati beberapa tahapan sebagai berikut :

1. Studi Pustaka/*literature*

   Tahapan ini dapat dilakukan dengan membaca artikel atau makalah penelitian yang terkait langsung dengan tugas akhir, dan melakukan penelitian setelah masalah yang akan dibahas sesuai dan relevan.

2. Perancangan Sistem

Pada tahap ini membahas bagaimana membangun metode dan menerapkannya pada sistem tugas akhir. Selain itu, apa yang digunakan dalam penelitian adalah perangkat lunak, kemudian bagaimana cara mengkonfigurasi metode pada tugas akhir atau menulis kode untuk penerapan metode tersebut.

3. Pengujian

Tahapan ini merupakan tahap pengujian metodologi penelitian dan penelitian sebelumnya guna mendapatkan data hasil pengujian yang sesuai dengan algoritma.

4. Analisa

Tahapan ini akan menganalisis data hasil pengujian dengan menerapkan metode tertentu sehingga akan diperoleh hasil yang obyektif dalam hal memperoleh data dari proses pengujian.

5. Kesimpulan dan Saran

Tahapan ini dilakukan melalui kesimpulan yang diambil dari analisis dan penelitian kepustakaan serta rekomendasi kepada penulis selanjutnya (jika dijadikan acuan), kemudia ditarik kesimpulan dari hasil penelitian.

1.6 Sistematika Penulisan

Adapun sistematika penulisan dalam Proposal Tugas Akhir ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Pada bab I akan berisikan Latar Belakang masalah, Tujuan, Manfaat, Perumusan Masalah, Batasan Masalah, Kemudian Metodologi Penelitian, dan Sistematikan Penulisan.

BAB II. TINJAUAN PUSTAKA

Pada Bab II akan berisi dasar teori *Malware*,*Jenis serangan malware, Malware analysis*, *Banking Malware*, *Android*, *Machine Learning*, *Feature Extraction*, *Feature Selection*, metode *Support Vector Machine (SVM),* Karakterisitik SVM, dan Evaluasi.

BAB III. ANALISIS DAN PERANCANGAN

Pada Bab III ini membahas analisis dan perancangan sistem klasifikasi serangan *Malware Banking* menggunakan metode *Support Vector Machine (SVM)*.

BAB IV. IMPLEMENTASI PENGUJIAN

Pada Bab IV membahas proses hasil pengklasifikasian dan serangan *Malware Banking* menggunakan metode *Support Vector Machine (SVM).*

BAB V. KESIMPULAN

Bab V ini berisi kesimpulan yang diambil dari setiap bab yang berhubungan dengan hasil implementasi metode support vector machine (SVM) untuk mengklasifikasikan serangan malware bank. Bab ini juga berisi saran-saran yang diharapkan dapat digunakan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] D. Xu, “Analysis of Mobile Banking Malware on the Android Operating System,” , pp. 1–104, 2017.

[2] S. Natalius, “Assessing the Role of Online Banking Characteristics in the Target Selection of the Banking Malware.” no. 61502134, pp. 833–838, 2018

[3] J. Sun, K. Yan, X. Liu, C. Yang, and Y. Fu, “Malware Detection on Android Smartphones using Keywords Vector and SVM,” no. 61502134, pp. 833–838, 2017.

[4] M. K. A. Abuthawabeh and K. W. Mahmoud, “Android Malware Detection and Categorization Based on Conversation-level Network Traffic Features,” pp. 42–47, 2019.

[5] S. R. Tiwari and R. U. Shukla, “An Android Malware Detection Technique using Optimized permission and API with PCA,” *2018 Second Int. Conf. Intell. Comput. Control Syst.*, pp. 2611–2616, 2018.

[6] W. Li, J. Ge, and G. Dai, “Detecting Malware for Android Platform : An SVM- based Approach,” pp. 464–469, 2015, doi: 10.1109/CSCloud.2015.50.

[7] N. Idika and A. P. Mathur, “A Survey of Malware Detection Techniques,” *SERC Tech. Reports*, 2007, [Online]. Available: http://www.serc.net/report/tr286.pdf.

[8] G. Cabau, M. Buhu, and C. P. Oprisa, “Malware classification based on dynamic behavior,” *Proc. - 18th Int. Symp. Symb. Numer. Algorithms Sci. Comput. SYNASC 2016*, pp. 315–318, 2017, doi: 10.1109/SYNASC.2016.057.

[9] M. Ijaz, M. H. Durad, and M. Ismail, “Static and Dynamic Malware Analysis Using Machine Learning,” *2019 16th Int. Bhurban Conf. Appl.*

Sci. Technol., pp. 687–691, 2019, doi: 10.1109/IBCAST.2019.8667136.

[10] E. Gandotra, D. Bansal, and S. Sofat, "Malware Analysis and Classification: A Survey," *J. Inf. Secur.*, vol. 05, no. 02, pp. 56–64, 2014, doi: 10.4236/jis.2014.52006.

[11] D. Arp, M. Spreitzenbarth, H. Malte, H. Gascon, and K. Rieck, "DREBIN : Effective and Explainable Detection of Android Malware in Your Pocket D REBIN : Effective and Explainable Detection of Android Malware in Your Pocket," , doi: 10.14722/ndss.2014.23247,2014.

[12] L. Taheri, A. Fitriah, A. Kadir, A. H. Lashkari, A. Fitriah, and A. H. L. Unb, "Extensible Android Malware Detection and Family Classification Using Network-Flows and API-Calls", 2019.

[13] P. Black, I. Gondal, and R. Layton, "A Survey of Similarities in Banking Malware Behaviours," doi: 10.1016/j.cose.2017.09.013,2017.

[14] B. H. M. Custers and R. L. D. Pool, "Banking malware and the laundering of its profits,"doi: 10.1177/1477370818788007,2018.

[15] G. Iadarola, F. Martinelli, F. Mercaldo, and A. Santone, "Formal Methods for Android Banking Malware Analysis and Detection," *2019 6th Int. Conf. Internet Things Syst. Manag. Secur. IOTSMS 2019*, pp. 331–336, 2019, doi: 10.1109/IOTSMS48152.2019.8939172.

[16] H. Siqueira and F. Barros, "A Feature Extraction Process for Sentiment Analysis of Opinions on Services." vol. 03, no. 01, pp. 26–44,2016.

[17] A. Fitriah and A. Kadir, "A Detection Framework for Android Financial Malware, vol. 06, no. 01, pp. 30–67" 2018.

[18] X. Liu, J. Tang, and S. Member, "Mass Classification in Mammograms Using.pdf," *IEEE Syst. J.*, vol. 8, no. 3, pp. 910–920, 2014, doi: 10.1109/JSYST.2013.2286539.

[19] S. Visalakshi and V. Radha, "A literature review of feature selection

techniques and applications: Review of feature selection in data mining," *2014 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2014*, no. 1997, 2015, doi: 10.1109/ICCIC.2014.7238499.

[20] M. Wadkar, F. Di Troia, and M. Stamp, "Detecting malware evolution using support vector machines," *Expert Syst. Appl.*, vol. 143, p. 113022, 2020, doi: 10.1016/j.eswa.2019.113022.

[21] A. K. Santra and C. J. Christy, "Genetic Algorithm and Confusion Matrix for Document Clustering 1," vol. 9, no. 1, pp. 322–328, 2012.