DETEKSI *MALWARE RANSOMWARE* PADA *PLATFORM ANDROID* MENGGUNAKAN METODE *RANDOM FOREST*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

RAHMAT FEBRIANSYAH
09011381722133

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

DETEKSI *MALWARE RANSOMWARE* PADA *PLATFORM ANDROID* MENGGUNAKAN METODE *RANDOM FOREST*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

Rahmat Febriansyah
09011381722133

Palembang, 10 Oktober 2021
Mengetahui,

Pembimbing Tugas Akhir	Ketua Jurusan Sistem Komputer
Ahmad Heryanto, S.Kom., M.T.	**Dr. Ir. H. Sukemi, M.T.**
NIP. 198701222015041002	**NIP. 196612032006041001**

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 P. P. Prasetya, S.Kom., M.T.**
3. **Penguji Sidang** : **Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing** : **Ahmad Heryanto, S.Kom., M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

UNIVERSITAS SRIWIJAYA FAKULTAS ILMU KOMPUTER JURUSAN SISTEM KOMPUTER

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

NIP. 196612032006041001

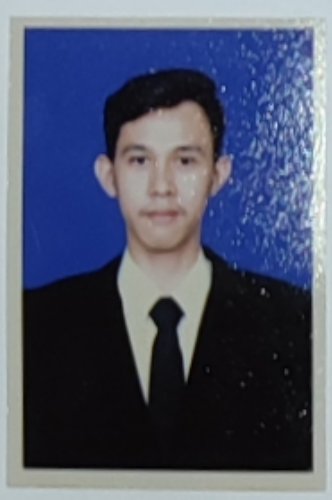
HALAMAN PERNYATAAN

Yang bertanda yangan dibawah ini:

Nama : Rahmat Febriansyah
NIM : 09011381722133
Program Studi : Sistem Komputer
Judul : Deteksi *Malware Ransomware* Pada *Platform Android* Menggunakan Metode *Random Forest*

Hasil pengecekan *Software iThentivate/Turnitin* : 14%

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, September 2021

Rahmat Febriansyah
09011381722133

MOTTO DAN PERSEMBAHAN

Motto :

Bukan Karena Kita Yang Hebat
Tetapi Karena Allah Yang Memudahkan

"Barangsiapa berjalan di suatu jalan untuk mencari ilmu, niscaya Allah akan memudahkan baginya jalan ke surga." (HR.Tirmidzi)

"Allah meninggikan orang-orang yang diberi ilmu atas orang-orang yang beriman beberapa derajat". (HR. Darimi)

Aku persembahkan untuk:

- **Kedua Orang tua ku tercinta, yang selalu memberikan dukungan moral, spiritual dan material yang tiada hentinya.**

- **adik dan kakak ku serta keluarga besar yang selalu memberi motivasi dan dukungan.**

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 ‘‘Deteksi *Malware Ransomware* Pada *Platform Android* Menggunakan Teknik *Random Forest*’’ dengan baik.

Dalam penelitian tugas akhir ini penulis menjelaskan mengenai pendeteksian *malware* jenis *ransomware* pada *platform android* dengan menggunakan teknik *random forest* berserta dengan data-data hasil penelitian yang saya lakukan. Harapan saya agar tulisan ini dapat bermanfaat serta menjadi penambah wawasan bagi pembaca.

Pada penulisan 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 terima kasih kepada :

1. Allah SWT Yang memberikan nikmat kemudahan, kesehatan dan kesempatan dalam melaksanakan tugas akhir ini.
2. Baginda Nabi Muhammad SAW sang suri tauladan.
3. Kedua orang tua, saudara, dan keluarga besar yang selalu mendoakan dan selalu memberikan motivasi, semangat serta support dalam hal moral, material dan spiritual.
4. Bapak Jaidan Jauhari, S.Pd. M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
5. Bapak Dr.Ir. H.Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya
6. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Bapak Ahmad Fali Oklilas, M.T. selaku dosen pembimbing akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

8. Seluruh Dosen, Staff dan karyawan Fakultas Ilmu Komputer Universitas Sriwijaya
9. Teman seperjuangan Kedal Squad yang selalu memberikan masukkan, motivasi dan semangat.
10. Pacarku yang selalu mensupport.
11. Teman-teman seperjuangan Sistem Komputer Angkatan 2017 Bukit yang selalu memberi dukungan.
12. Dan semua kerabat yang telah memberikan dukungan dan semangat 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 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.

Sebagai penutup, semoga tugas akhir ini akan menjadi tambahan ilmu pengetahuan serta menambah wawasan kita dan bagi mahasiswa yang membutuhkan khususnya mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya serta memberi manfaat bagi semua yang membaca. Sebelum dan sesudahnya saya mengucapkan terimakasih.

Palembang, April 2021

Penulis

Rahmat Febriansyah

09011381722133

DETEKSI *MALWARE RANSOMWARE* PADA *PLATFORM ANDROID* MENGGUNAKAN METODE *RANDOM FOREST*

RAHMAT FEBRIANSYAH (09011381722133)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Univesitas Sriwijaya
Email : rahmat932016@gmail.com

ABSTRAK

Malicious Software atau yang lebih dikenal dengan *Malware* merupakan suatu perangkat lunak yang dapat masuk dan menyerang ke dalam suatu sistem operasi yang mana dapat menyebabkan kerusakan pada sistem operasi tersebut[1]. Malware itu sendiri terdiri dari banyak jenis, ada beberapa jenis *Malware* yang umum diketauhi oleh khalayak ramai, misalnya ada *Malware Trojan, Malware Ransomware, Malware spyware, Malware Adware, Worm* dan ada masih banyak jenis-jenis lainnya. Pada penelitian ini jenis malware yang digunakan adalah *Ransomware*. *Malware ransomware* ini dapat menyerang berbagai macam sistem operasi misalnya saja *Android*. *Android* itu sendiri merupakan salah satu dari banyak sistem operasi yang ada pada perangkat seluler yang bersifat *open source* serta di dalam nya memiliki banyak fitur yang lengkap. Dikarenakan *Android* ini adalah sebuah sistem operasi yang sifatnya *open source*, maka banyak *vendor* dan berbagai merk telepon seluler memilih untuk menggunakan sistem operasi ini[3]. Untuk mendeteksi *malware ransomware* ini penulis menggunakan *Machine Learning* dimana pada penelitian ini metode yang digunakan adalah algortima *Random Forest* yang menghasilkan akurasi sebesar 91,75%.

Kata Kunci : Malware, Ransomware, Deteksi, *Android, Random Forest, Machine Learning.*

DETECTION OF RANSOMWARE MALWARE ON THE ANDROID PLATFORM USING RANDOM FOREST METHOD

RAHMAT FEBRIANSYAH (09011381722133)
Departement of Computer Engineering, Faculty of Computer Science, Sriwijaya University
Email : rahmat932016@gmail.com

ABSTRACT

Malicious Software or better known as *Malware* is software that can enter and attack an operating system which can cause damage to the operating system. *Malware* itself consists of many types, there are several types of *Malware* that are commonly known by the general public, for example there are *Trojan Malware, Ransomware Malware, Spyware Malware, Adware Malware, Worms* and there are many other types. In this study, the type of *malware* used is *Ransomware*. This *ransomware malware* can attack various operating systems, such as *Android*. *Android* itself is one of the many operating systems available on mobile devices that are open source and have many complete features. Because *Android* is an operating system that is open source, many vendors and various brands of cellular phones choose to use this operating system. To detect this *ransomware malware,* the author uses *Machine Learning* where in this study the method used is the *Random Forest* algorithm which produces an accuracy of 91.75%.

Keywords : *Malware, Ransomware, Detection, Android, Random Forest, Machine Learning.*

DAFTAR ISI

Halaman

BAB III METODOLOGI PENELITIAN

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1. Latar Belakang

Malicious Software atau yang lebih dikenal dengan *Malware* merupakan suatu perangkat lunak yang dapat masuk dan menyerang ke dalam suatu sistem operasi yang mana dapat menyebabkan kerusakan pada sistem operasi tersebut[1]. Pada masa sekarang, para *hacker* atau penyerang menggunakan berbagai macam cara untuk membuat dan menghasilkan jenis *malware* baru yang bisa mereka gunakan untuk mencari keuntungan. Salah satu jenis malware yang baru-baru ini menyebar adalah *ransomware*[2]. *Malware ransomware* ini dapat menyerang berbagai macam sistem operasi misalnya saja *Android*.

Android merupakan salah satu dari banyak sistem operasi yang ada pada perangkat seluler yang bersifat *open source* serta di dalam nya memiliki banyak fitur yang lengkap. Dikarenakan *Android* ini adalah sebuah sistem operas yang sifatnya *open source*, maka banyak *vendor* dan berbagai merk telepon seluler memilih untuk menggunakan sistem operasi ini. Malware itu sendiri terdiri dari banyak jenis, ada beberapa jenis *Malware* yang umum diketauhi oleh khalayak ramai, misalnya ada *Malware Trojan, Malware Ransomware, Malware spyware, Malware Adware, Worm* ada masih banyak jenis-jenis lainnya[3].

Andorid malware itu sendiri merupakan sebuah perangkat lunak yang berbahaya dimana tujuan diciptakannya adalah untuk menyerang sistem operasi *Android* pada *Smartphone*. Penyerangan terhadap sistem operasi *Android* ini dapat menyebabkan pengguna *Android* tersebut mengalami kebocoran informasi yang bersifat pribadi dan rahasia[4].

Untuk mendeteksi *malware ransomware* ini ada banyak metode yang bisa digunakan, misalnya dengan menggunakan metode anlisis *static* dan *dynamic*, kemudian bisa juga dengan menggunakan *Machine Learning*. pada

penelitian ini metode yang digunakan adalah *Machine Learning* dimana salah satu algoritma yang bisa digunakan adalah algortima *Random Forest.*

Random forest adalah sebuah metode yang membangkitkan sejumlah pohon klasifikasi. Metode *random forest* ini salah satu kelebihannya adalah dapat meningkatkan hasil akurasi, yaitu dengan cara membangkitkan simpul anak untuk setiap simpul diatasnya kemudian dilakukan sebuah pemilihan secara random atau acak[5]. Metode ini sudah sering digunakan dalam banyak penelitian-penelitian sebelumya.

Penelitian mengenai deteksi maupun klasifikasi malware ini sudah banyak dilakukan sebelumnya tentu saja dengan metode dan jenis malware yang berbeda-beda, dimana diantara nya adalah penelitian yang sudah dilakukan oleh Fahron pada tahun 2019 dengan judul penelitian 'Klasifikasi *Trojan Ransomware* Berdasarkan Karakter Menggunakan Algoritma *Naïve Bayes Classifier*'. Pada penelitian yang menggunakan algortima *Naïve Bayes Classifier* tersebut hasil akurasi dari penelitian yang dilakukan adalah sebesar 73,26%[6]. Kemudian ada juga penelitian yang sudah dilakukan oleh Sendi Herlambang pada tahun 2018 dengan judul 'Deteksi *Malware Android* Berdasarkan *System Call* Menggunakan *Support Vector Machine (SVM)'*. Dengan menggunakan metode *SVM* penelitian tersebut mendapat hasil akurasi sebesar 73.3%[7]. Selanjutnya ada juga penelitian yang sudah dilakukan oleh Inda Anggraini pada tahun 2019 dengan judul penelitian 'Penerapan *Naïve Bayes* Pada Pendeteksian *Malware* Dengan Diskritisasi Variabel'. Pada penelitian tesebut akurasi yang didapat adalah sebesar 69,72%[8]. Dapat dilihat dari 3 penelitian terdahulu diatas bahwa hasil akurasi yang didapat setelah dilakukan penelitian semuanya kurang dari 80%.

Dalam melakukan penelitian ini saya menggunakan metode yang berbeda dari ke-tiga penelitian terdahulu di atas yaitu menggunakan metode *random forest*, dimana metode ini memiliki beberapa keunggulan misalnya metode ini dapat memproses data dalam jumlah yang besar, kemudian metode ini juga dapat digunakan untuk mengatasi *noise-noise* dan *missing value* pada data yang digunakan. Metode *random forest* ini juga dapat melakukan *training*

data dengan efisien tanpa harus melakukan *scaling* data atau penskalaan data terlebih dahulu sehingga tidak memerlukan proses yang panjang. *Random forest* melakukan prediksi dengan cara *vote* atau pemilihan suara menggunakan pohon keputusan atau *Decision Tree* untuk mencari hasil prediksi. Hasil prediksi diambil berdasarkan *vote* dimana yang mendapat *vote* terbanyak merupakan pemenangnya sehingga hasil akurasi prediksi yang didapatkan akan lebih akurat[2]. Berdasarkan paparan tersebut, diharapkan hasil akurasi prediksi pada penelitian ini akan lebih baik jika dibanding dengan penelitian sebelumnya yang menggunakan metode berbeda dari penelitian ini.

2. Perumusan Masalah

Berdasarkan paparan pada bagian latar belakang diatas, maka dapat diambil rumusan masalah yaitu:

1. Bagaimana menerapkan algoritma *Random Forest* dalam mendeteksi *malware* jenis *ransomware* pada *platform Android*?.
2. Bagaimana mendapatkan hasil akurasi yang baik dalam mendeteksi *malware* jenis *ransomware* pada *platform Android* dengan algoritma *Random Forest*?

3. Batasan Masalah

Dalam proses penelitian ini ada beberapa batasan masalah yang diterapkan, yaitu:

1. Deteksi *malware* hanya jenis *ransomware*.
2. Algortima yang digunakan dalam mendeteksi *malware* jenis *ransomware* hanya menggunakan algortima *Random Forest*.
3. Penelitian mengguanakan *dataset CICAndMal2017*.
4. Jenis *ransomware* yang digunakan dari dataset adalah *porndroid.*
5. Program yang digunakan adalah *Jupyter Notebook*.

4. Tujuan Penelitian

Berdasarkan perumusan masalah yang telah dipaparkan diatas maka dapat disimpulkan bahwa tujuan dari dilakukannya penelitian ini adalah untuk menerapkan algoritma *Random Forest* dalam mendeteksi *ransomware* pada *platform Android*.

5. Manfaat Penelitian

Adapun manfaat dari dilakukannya penelitian adalah untuk mengetahui bagaimana cara menerapkan algoritma *Random Forest* dalam melakukan pendeteksian terhadap *Ransomware* pada *Platform Android*.

6. Metodologi Penelitian

Adapun metodologi penelitian yang dipakai dalam melakukan penelitian ini melewati beberapa tahapan, yaitu:

1. Tahap pertama (perumusan masalah)

   Tahap ini adalah dimana penulis menentukan pokok inti permasalahan mengenai deteksi *malware ransomware android*.

2. Tahap kedua (studi pustaka/*literature*)

   Pada tahap kedua ini penulis mencari referensi yang dapat diambil dari berbagai sumbel baik itu bersumber dari buku maupun yang bersumber jurnal yang tentunya ber dengan penelitian yang akan digunakan untuk menyelesaikan rumusan masalah pada *subbab* sebelumnya. Referensi yang digunakan berdasarkan kata kunci penelitian yang dilakukan.

3. Tahap ketiga (perancangan)

   Pada tahap ketiga ini membahas tentang rancangan jalannya proses penelitian berdasarkan rumusan masalah yang sudah ditentukan dan literatur yang digunakan.

4. Tahap keempat (pengujian)

Tahap ini adalah tahap pengujian algoritma dan *source code* yang telah dibuat untuk mendapatkan hasil persentasi akurasi deteksi *malware ransomware*.

5. Tahap kelima (analisis)

Tahap analisis ini merupakan tahap pengambilan data yang sudah diproses dan menganalisa untuk mendapatkan hasil dari penelitian.

6. Kesimpulan dan saran

Tahap ini penulis menarik kesimpulan berdasarkan proses dan hasil analisa penelitian serta saran untuk penelitian selanjutnya jika akan dijadikan bahan referensi.

7. Sistematika Penulisan

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

BAB I PENDAHULUAN

Bab pertama ini membahas tentang penjabaran secara sistematis topik yang diambil yang terdiri dari latar belakang, perumusan msalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi yang digunakan serta sistematika penulisan.

BAB II TIJAUAN PUSTAKA

Bab kedua ini menjelaskan dasar-dasar teori yang berhubungan dengan pokok pembahasan dari penelitian ini. Dasar teori ini berisi tentang malware dll, metode yang digunakan.

BAB III METODOLOGI PENELITIAN

Bab ketiga ini membahas mengenai tahapan-tahapan penelitian yang meliputi pengolahan data, pengujian serta analisis.

BAB IV HASIL DAN ANALISIS

Bab keempat ini berisi penjelasan mengenai proses dan hasil penelitian serta analisa terhadap penelitian yang telah dilakukan.

BAB V KESIMPULAN

Bab kelima ini berisi kesimpulan dan saran berdasarkan hasil analisa terhadap penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] A. S. Rusdi, N. Widiyasono, and H. Sulastri, "Analisis Infeksi Malware Pada Perangkat Android Dengan Metode Hybrid Analysis," no. 24, 2019.

[2] B. M. Khammas, "Ransomware Detection using Random Forest Technique," *ICT Express*, vol. 6, no. 4, pp. 325–331, 2020.

[3] S. Sinambela, A. R. Pangestu, and R. Feriyanto, "Analisis Aplikasi Malware pada Android dengan Metode Statik," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 3, no. 2, pp. 88–94, 2020.

[4] M. Sapti, "ANALISIS MALWARE PADA SISTEM OPERASI ANDROID MENGGUNAKAN PERMISSION-BASED," *Kemamp. Koneksi Mat. (Tinjauan Terhadap Pendekatan Pembelajaran Savi)*, vol. 53, no. 9, pp. 1689–1699, 2019.

[5] G. A. Sandag, "Prediksi Rating Aplikasi App Store Menggunakan Algoritma Random Forest," *CogITo Smart J.*, vol. 6, no. 2, p. 167, 2020.

[6] J. S. Komputer, F. I. Komputer, and U. Sriwijaya, "KLASIFIKASI TROJAN RANSOMWARE," 2019.

[7] 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.

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

[9] V. Rahmayanti *et al.*, "KLASIFIKASI MALWARE FAMILY MENGGUNAKAN METODE K-NEAREST NEIGHBOR," pp. 319–323, 2020.

[10] E. Tansen and D. W. Nurdiarto, "Analisis Dan Deteksi Malware Dengan Metode Hybrid Analysis Menggunakan Framework Mobsf," vol. 4, no. 2, pp. 191–201, 2020.

[11] Y. Makasudede, "Bab 2 tinjauan pustaka," pp. 8–45, 1953.

[12] "Perangkat pemeras," no. May 2016, p. 16444004, 2020.

[13] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," *Proc. - Int. Conf. Distrib. Comput. Syst.*, vol. 2016-Augus, pp. 303–312, 2016.

[14] P. Y. Pawar, Y. Gudhka, M. Sutar, and P. Godhani, "Android Malware Detection by Using Random Forest Algorithm," vol. 6, no. 4, pp. 2406–2408, 2020.

[15] D. Fransiska Amalia Kurniawan, “Analisis dan Implementasi Random Forest dan Regression Tree (CART) Untuk Klasifikasi pada Misuse Intrussion Detection System,” *Fak. Tek. Inform.*, no. Data Mining, pp. 1–7, 2011.

[16] 2019 Haines et al, A. goleman, daniel; boyatzis, Richard; Mckee, 2019 Haines et al, A. goleman, daniel; boyatzis, Richard; Mckee, 2019 Haines et al, and A. goleman, daniel; boyatzis, Richard; Mckee, “Penerapan Machine Learning,” *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2019.

[17] Handa Gustiawan, “No TitleΕΛΕΝΗ,” *Αγαη*, vol. 8, no. 5, p. 55, 2019.

[18] Y. L. Pavlov, “Random forests,” *Random For.*, pp. 1–122, 2019.

[19] 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.

[20] E. Table, “Confusion Matrix,” *SpringerReference*, 2012.

[21] H. A. Alatwi, “Android Malware Detection Using Category-Based Machine Learning Classifiers Rochester Institute of Technology Android Malware Detection Using Category-Based Machine Learning Classifiers,” 2016.

[22] N. Hardianto, “KLASIFIKASI ADWARE MALWARE PADA ANDROID,” 2020.

[23] A. P. Wibawa, M. G. A. Purnama, M. F. Akbar, and F. A. Dwiyanto, “Metode-metode Klasifikasi,” *Pros. Semin. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 1, pp. 134–138, 2018.