1. PENDAHULUAN

1.1. Latar Belakang

Dalam era perkembangan teknologi informasi dan komputer yang terus meningkat, tantangan keamanan semakin kompleks dengan adanya upaya penyamaran dalam bentuk obfuscated malware. Obfuscated malware merupakan bentuk perangkat lunak berbahaya yang cerdik dan menggunakan sejumlah teknik, seperti penggunaan enkripsi dan penyembunyian kode, dengan tujuan menyamarkan sifat asli perangkat lunak tersebut [28]. Kelompok malware, seperti Trojan, Spyware, dan Ransomware, telah menjadi fokus utama, mengubah kode sumber mereka agar sulit dikenali oleh deteksi tradisional. Sebagai contoh, Trojan menyamar sebagai aplikasi benign, mengecoh pengguna yang mengunduhnya dengan harapan mendapatkan perangkat lunak berguna [5]. Spyware menyusup dalam aplikasi bersih untuk mencuri informasi tanpa sepengetahuan pengguna[6], sedangkan Ransomware membatasi akses ke informasi penting dengan tuntutan tebusan[7]. Secara keseluruhan, ketiga jenis obfuscated malware saling terhubung, dimana nantinya Trojan digunakan untuk menyusupkan Spyware dan Ransomware ke dalam perangkat korban. Spyware kemudian menggali informasi terkait korban, sedangkan Ransomware, setelah memahami informasi tersebut dari Spyware, melakukan pembatasan akses ke data penting dengan harapan mencapai tujuannya setelah tuntutan pemerasan dikabulkan, data korban mungkin akan dilepas.

Dalam upaya mendeteksi obfuscated malware, sejumlah metode telah diajukan dan dinilai melalui berbagai penelitian dengan menggunakan Metode Pembelajaran Mesin Random Forest [23], Decision Tree [24], Extra Trees [25], CNN [26], dan Metode lainnya. Meskipun penelitian terkait deteksi obfuscated malware sudah meluas, penerapan pendekatan Deep Neural Decision Forest (DNDF) masih terbatas, dikarenakan kurangnya eksplorasi mendalam terhadap potensinya dalam mengatasi kompleksitas dan ketangguhan obfuscated malware. Oleh karena itu, penelitian lebih lanjut mengenai implementasi metode DNDF diusulkan sebagai langkah inovatif untuk menjelajahi solusi deteksi obfuscated malware.

Penggabungan model Decision Trees dengan deep neural network diusulkan sebagai solusi yang dapat bersaing dalam mendeteksi obfuscated malware. Decision Trees menonjol dengan keputusan yang mudah diinterpretasikan dan pemilihan fitur yang alami, sementara deep neural network unggul dalam mengekstraksi pola kompleks dan menangani relasi yang lebih abstrak. Integrasi keduanya diharapkan memberikan model dengan tingkat akurasi yang dapat bersaing dengan model yang telah ada, menjaga keseimbangan antara performa dan interpretabilitas. Penggabungan teknik deep learning dengan kemudahan pemahaman dan kemampuan gabungan dari model decision forest. Hal ini memungkinkan DNDF untuk mengekstraksi atribut dan pola yang kompleks [2].

Pemilihan 10-fold cross-validation dalam penelitian ini dilatarbelakangi oleh keinginan untuk memberikan evaluasi yang kokoh terhadap kinerja model, terutama dalam mengatasi variasi data, keseimbangan, dan keterbatasan dataset yang perlu diperhitungkan [3]. Metode ini diharapkan memberikan estimasi kinerja yang stabil, mampu mengatasi fluktuasi, serta memberikan wawasan menyeluruh terhadap kemampuan model dalam menanggapi variasi dalam dataset sesuai dengan tujuan penelitian.

Selain itu, keunggulan pelatihan Extra Trees yang kurang tergantung pada distribusi sampel dan kemampuan algoritma ini dalam melakukan pemilihan fitur secara alami melalui pembangunan beberapa pohon sangat bermanfaat, terutama dalam situasi di mana dataset bersifat tidak seimbang atau beberapa kelas kurang terwakili. Kelebihan ini dapat mendukung identifikasi fitur-fitur yang paling relevan untuk memprediksi malware yang tersembunyi, meningkatkan ketepatan dan ketangguhan model [4]. Oleh karena itu, penggunaan Extra Trees dalam konteks pemodelan deteksi obfuscated malware pada penelitian ini dapat menjadi pilihan yang cerdas.

1.2. Perumusan Masalah

Dengan latar belakang tersebut, dapat disimpulkan bahwa rumusan masalah dalam penelitian ini mencakup:

- Bagaimana model "Neural Decision Forest" dengan metode Feature Selection "Extra Trees Classifier" dapat mendeteksi obfuscated malware?
- Bagaimana performansi dari model "Neural Decision Forest" dengan metode Feature Selection "Extra Trees Classifier" dalam mendeteksi obfuscated malware?

1.3. Tujuan

Dengan rumusan masalah tersebut, dapat disimpulkan bahwa tujuan dari penelitian ini mencakup:

- Menerapkan dan menganalisis efektivitas model "Neural Decision Forest" dengan metode Feature Selection "Extra Trees Classifier" dalam mendeteksi obfuscated malware.
- Mengevaluasi kinerja model yang dibuat dengan menggunakan metrik yang relevan, dengan tujuan untuk memberikan analisis mendalam terhadap hasil penelitian.

1.4. Hipotesis

Penerapan model "Neural Decision Forest" dengan menggunakan metode seleksi fitur "Extra Trees Classifier" akan menjadi salah satu pendekatan yang efektif untuk mendeteksi obfuscated malware pada dataset Malware Memory Analysis CIC-MalMem-2022. Pemilihan model ini didasarkan pada kemampuan neural network untuk mengenali pola kompleks dalam data, sementara penggunaan Extra Trees Classifier sebagai metode seleksi fitur diharapkan dapat meningkatkan ketepatan dalam mengidentifikasi fitur yang relevan untuk deteksi malware. hipotesa sementara ini menunjukkan potensi untuk menghasilkan pendekatan yang dapat bersaing. Dengan mengadopsi pendekatan ini, hipotesa menyiratkan bahwa hasil eksperimen dapat mencapai tingkat akurasi deteksi yang bersaing, memberikan kontribusi berharga dalam pemahaman dan penanganan obfuscated malware pada konteks dataset khusus ini.

1.5. Rencana Kegiatan

Dalam rencana kegiatan ini, langkah-langkah yang akan diambil mencakup:

1. Kajian Pustaka:
    - Melakukan tinjauan pustaka terkait obfuscated malware detection, terutama fokus pada metode "Neural Decision Forest" dan Feature Selection "Extra Trees Classifier".
    - Meneliti penelitian-penelitian terkini yang mengaplikasikan model serupa.
2. Pengumpulan Data:
    - Menggunakan dataset Malware Memory Analysis CIC-MalMem-2022 sebagai basis data untuk penelitian.
    - Menggali informasi mengenai Trojan, Spyware, dan Ransomware dalam dataset tersebut.
3. Rancangan Penelitian:
    - Mengembangkan model "Neural Decision Forest" dengan metode Feature Selection "Extra Trees Classifier" menggunakan platform Jupyter Notebook.
    - Merancang eksperimen dengan memperhatikan prosedur penelitian yang memastikan validitas dan reliabilitas hasil.
4. Pengembangan Sistem:
    - Menerapkan model menggunakan Jupyter Notebook dengan memperhatikan prinsip-prinsip pemrograman terbaik.
    - Melakukan iterasi dan pengembangan model untuk meningkatkan performa.
5. Pengujian Hasil Penelitian:
    - Menggunakan 10-fold cross-validation untuk menguji model.
    - Menganalisis hasil, melakukan penafsiran terhadap performa model, dan menyimpulkan temuan penelitian.

Dengan rencana kegiatan ini, diharapkan Tugas Akhir dapat dilaksanakan secara sistematis dan menghasilkan kontribusi dalam deteksi obfuscated malware menggunakan model "Neural Decision Forest" dengan metode Feature Selection "Extra Trees Classifier".

1.6. Jadwal Kegiatan

Kegiatan	Bulan					
	1	2	3	4	5	6
Kajian Pustaka						
Pengumpulan Data						
Perancangangan Penelitian						
Pengembangan Sistem						
Pengujian Hasil Penelitian						