

INTISARI

PENILAIAN RISIKO *MALWARE* ANDROID MENGGUNAKAN KLASIFIKASI FUZZY DAN PARAMETER *LIKELIHOOD*

Nikita Christy Alfeana

21/477040/SV/19145

Ancaman *malware* pada perangkat Android terus meningkat seiring dengan bertambahnya pengguna mobile. Deteksi multi-engine, seperti VirusTotal dan ReversingLabs, digunakan untuk mengidentifikasi *malware*, tetapi hasil deteksi sering kali berupa skor yang sulit diinterpretasikan dan menyisakan ambiguitas. Penelitian ini bertujuan untuk mengembangkan model penilaian risiko berbasis pendekatan fuzzy dengan parameter *likelihood* untuk mengurangi ambiguitas tersebut. Model ini menggabungkan hasil deteksi dari VirusTotal dan ReversingLabs, serta menggunakan metode fuzzy untuk menghasilkan penilaian risiko yang lebih bermakna.

Penelitian ini menggunakan metode eksperimen kuantitatif yang melibatkan tahapan kalkulasi sistem fuzzy, eksplorasi parameter, dan penggabungan hasil deteksi dari multi-engine. Dataset yang digunakan terdiri dari 1000 *malware* yang diekstrak dari *MalwareBazaar* dan dianalisis dengan menggunakan platform VirusTotal dan ReversingLabs. Hasil deteksi dari kedua platform tersebut kemudian diproses dengan pemodelan fuzzy melalui skrip Python. Output akhir dari model ini berupa penilaian risiko *malware* yang dikategorikan ke dalam lima tingkat, yaitu *Very Unlikely*, *Unlikely*, *Possible*, *Likely*, dan *Very Likely*.

Hasil penelitian menunjukkan bahwa model fuzzy dapat mengurangi ambiguitas interpretasi dan menghasilkan klasifikasi risiko yang lebih efektif, dengan korelasi yang tinggi terhadap hasil deteksi VirusTotal (0,92) dan ReversingLabs (0,96). Kombinasi kedua platform ini menghasilkan penilaian risiko *malware* yang lebih optimal, mempermudah analisis tren risiko, dan meningkatkan keandalan penilaian risiko. Penelitian ini memberikan kontribusi dalam penilaian risiko *malware* pada perangkat Android melalui pendekatan yang lebih terukur dan interpretatif.

Kata Kunci: Ancaman Android, *Malware*, *Multi-engine Detection*, *Fuzzy Logic*, *Risk Assessment*, Parameter *Likelihood*.

ABSTRACT

ANDROID MALWARE RISK ASSESSMENT USING FUZZY CLASSIFICATION TO SUPPORT DECISION-MAKING

Nikita Christy Alfeana

21/477040/SV/19145

The threat of malware on Android devices continues to rise with the increasing number of mobile users. Multi-engine detection systems, such as VirusTotal and ReversingLabs, are used to identify malware; however, the detection results often consist of scores that are difficult to interpret, leading to ambiguity. This study aims to develop a risk assessment model based on a fuzzy approach with likelihood parameters to reduce such ambiguity. The model integrates detection results from VirusTotal and ReversingLabs, utilizing fuzzy methods to produce more meaningful risk assessments.

This research employs a quantitative experimental method involving fuzzy system calculations, parameter exploration, and the integration of multi-engine detection results. The dataset used consists of 1000 malware samples extracted from MalwareBazaar, which were analyzed using the VirusTotal and ReversingLabs platforms. The detection results from both platforms were processed through fuzzy modeling using Python scripts. The final output of the model is a malware risk assessment categorized into five levels: Very Unlikely, Unlikely, Possible, Likely, and Very Likely.

The results of the study demonstrate that the fuzzy model effectively reduces interpretative ambiguity and provides more effective risk classification, with high correlations to the detection results of VirusTotal (0.92) and ReversingLabs (0.96). The combination of these two platforms yields an optimized malware risk assessment, facilitates risk trend analysis, and enhances the reliability of risk evaluation. This research contributes to the development of a more measured and interpretable approach to malware risk assessment on Android devices.

Keywords: *Android Threat, Malware, Multi-engine Detection, Fuzzy Logic, Risk Assessment, Likelihood*