

**PENERAPAN METODE *IMPROVED RANDOM FOREST* DAN ALGORITMA C4.5
SEBAGAI *CLASSIFIER* UNTUK MENDETEKSI *RANSOMWARE* BERDASARKAN
FREKUENSI KEMUNCULAN *API CALLS***

M. Rozin Anjad
(160411100037)

Dosen Pembimbing 1 : Dwi Kuswanto S.Pd., M.T
Dosen Pembimbing 2 : Husni S.Kom., M.Kom

ABSTRAK

Teknik *Signature base* tidak dapat mengenali *ransomware* jenis baru tanpa di analisis terlebih dahulu. Untuk itu diperlukan teknik mendeteksi *ransomware* menggunakan machine learning. Penelitian ini bertujuan menerapkan metode *improved random forest* untuk mendeteksi *ransomware*. *Improved Random forest* merupakan *Random forest* yang dipakai menggunakan *feature evaluator* dan *instance filter* untuk meningkatkan akurasi dari *random forest* biasa. Penelitian ini akan menggunakan metode *improved random forest* dengan algoritma *c4.5* sebagai *classifier* untuk mendeteksi *ransomware*. Pada penelitian ini ada beberapa tahap yang dilakukan untuk mendeteksi malware menggunakan *improved random forest* yaitu mengekstrak *api calls*, kemudian memilih fitur berdasarkan rasio kemunculan pada malware, melakukan *fitur evaluator* dan resampling kemudian mengklasifikasikannya. Fitur yang digunakan ialah *API calls* yang ada dalam malware berdasarkan frekuensi yang paling banyak muncul. Berdasarkan pengujian yang telah dilakukan, *api call* sebagai fitur sangat berpengaruh pada tingkat akurasi. Dimana *improved random forest* mampu mendeteksi *ransomware* dengan baik berdasarkan *api calls* sebagai fitur dan dengan akurasi sebesar 96%. Hal ini dikarenakan nilai rasio kemunculan yang digunakan kecil yaitu 0.02 sehingga fitur yang digunakan sebanyak 188 lebih baik.

Kata Kunci : *Ransomware, api call, Improved Random forest, Algoritma C4.5.*

APPLICATION OF IMPROVED RANDOM FOREST METHOD AND C4.5 ALGORITHM AS A CLASSIFIER TO DETECT RANSOMWARE BASED ON FREQUENCY OF API CALLS

M. Rozin Anjad
(160411100037)

Dosen Pembimbing 1 : Dwi Kuswanto S.Pd., M.T
Dosen Pembimbing 2 : Husni S.Kom., M.Kom

ABSTRACT

The *signature base* technique cannot identify new types of ransomware without first analyzing it. This requires a technique to detect ransomware using *machine learning*. This study aims to apply an improved random forest method to detect *ransomware*. *Improved random forest* is a *random forest* that is used using the *evaluator feature* and filter instances to increase the accuracy of the regular random forest. This study will use an *improved random forest* method with the *c4.5 algorithm* as a classifier to detect ransomware. In this study there are several steps taken to detect malware using an improved *random forest*, namely extracting api calls, then selecting features based on the appearance ratio of the *malware*, performing an evaluator and resampling feature and then classifying them. The feature used is the API calls in the malware based on the frequency that occurs the most. Based on the tests that have been done, the api call as a feature has a big effect on the level of accuracy. Where the *improved random forest* was able to properly detect ransomware based on api calls as a feature and with an accuracy of 96%. This is because the appearance ratio value used is small, namely 0.02, so the features used are 188 better. **Keywords:** *Ransomware, api call, Improved Random forest, C4.5 Algorithm.*