<table>
<tr><td rowspan="2"><b>cases</b></td><td><b>doc_1</b></td><td><b>doc_2</b></td><td><b>decision</b></td><td><b>id</b></td></tr>
<tr>
<td>
<table>
<tr><td><b>authors</b></td><td>Javad Hassannataj Joloudari
Mojtaba Haderbadi
Amir Mashmool
Mohammad GhasemiGol
Shahab S. Band
Amir Mosavi</td></tr>
<tr><td><b>title</b></td><td>Early detection of the advanced persistent threat attack using performance analysis of deep learning</td></tr>
<tr><td><b>publication_date</b></td><td>2020-01-01 00:00:00</td></tr>
<tr><td><b>source</b></td><td>SupportedSources.INTERNET_ARCHIVE</td></tr>
<tr><td><b>journal</b></td><td>Institute of Electrical and Electronics Engineers (IEEE)</td></tr>
<tr><td><b>volume</b></td><td></td></tr>
<tr><td><b>doi</b></td><td>10.1109/access.2020.3029202</td></tr>
<tr><td><b>urls</b></td><td>https://web.archive.org/web/20201007065139/https://ieeexplore.ieee.org/ielx7/6287639/6514899/09214817.pdf?tp=&arnumber=9214817&isnumber=6514899&ref=</td></tr>
<tr><td><b>id</b></td><td>id-8620917455227446775</td></tr>
<tr><td><b>abstract</b></td><td></td></tr>
<tr><td><b>versions</b></td><td></td></tr>
</table>
</td>
<td>
<table>
<tr><td><b>authors</b></td><td>Javad Hassannataj Joloudari
Mojtaba Haderbadi
Amir Mashmool
Mohammad GhasemiGol
Shahab S.
Amir Mosavi</td></tr>
<tr><td><b>title</b></td><td>Early detection of the advanced persistent threat attack using performance analysis of deep learning</td></tr>
<tr><td><b>publication_date</b></td><td>2020-09-19 00:00:00</td></tr>
<tr><td><b>source</b></td><td>SupportedSources.INTERNET_ARCHIVE</td></tr>
<tr><td><b>journal</b></td><td></td></tr>
<tr><td><b>volume</b></td><td></td></tr>
<tr><td><b>doi</b></td><td></td></tr>
<tr><td><b>urls</b></td><td>https://web.archive.org/web/20200929002143/https://arxiv.org/ftp/arxiv/papers/2009/2009.10524.pdf</td></tr>
<tr><td><b>id</b></td><td>id3194661624927250302</td></tr>
<tr><td><b>abstract</b></td><td>One of the most common and important destructive attacks on the victim system is Advanced Persistent Threat (APT)-attack. The APT attacker can achieve his hostile goals by obtaining information and gaining financial benefits regarding the infrastructure of a network. One of the solutions to detect a secret APT attack is using network traffic. Due to the nature of the APT attack in terms of being on the network for a long time and the fact that the network may crash because of high traffic, it is difficult to detect this type of attack. Hence, in this study, machine learning methods such as C5.0 decision tree, Bayesian network and deep neural network are used for timely detection and classification of APT-attacks on the NSL-KDD dataset. Moreover, 10-fold cross validation method is used to experiment these models. As a result, the accuracy (ACC) of the C5.0 decision tree, Bayesian network and 6-layer deep learning models is obtained as 95.64%, 88.37% and 98.85%, respectively, and also, in terms of the important criterion of the false positive rate (FPR), the FPR value for the C5.0 decision tree, Bayesian network and 6-layer deep learning models is obtained as 2.56, 10.47 and 1.13, respectively. Other criterions such as sensitivity, specificity, accuracy, false negative rate and F-measure are also investigated for the models, and the experimental results show that the deep learning model with automatic multi-layered extraction of features has the best performance for timely detection of an APT-attack comparing to other classification models.</td></tr>
<tr><td><b>versions</b></td><td></td></tr>
</table>
</td>
<td>DUPLICATES</td>
<td>124</td>
</tr>
</table>