

# Intelligent Threat Detection A4:

# Yousef Al-Taher

# 20190029

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Training | Testing | | | | | | | | | | |
| Model | Accuracy | Accuracy | Precision | | | Recall | | | F-Score | | | AUC |
| C1 | C2 | C3 | C1 | C2 | C3 | C1 | C2 | C3 |
| Log Reg | 0.8306 | 0.8334 | 0.85 | 0 | 0.53 | 0.97 | 0 | 0.17 | 0.91 | 0 | 0.25 | 0.766 |
| DT | 0.9943 | 0.7426 | 0.86 | 0.03 | 0.28 | 0.84 | 0.04 | 0.31 | 0.85 | 0.03 | 0.30 | 0.561 |
| RF | 0.9943 | 0.8245 | 0.85 | 0 | 0.46 | 0.96 | 0.00 | 0.18 | 0.90 | 0.00 | 0.26 | 0.719 |
| KNN | 0.8569 | 0.8161 | 0.85 | 0.01 | 0.41 | 0.95 | 0.00 | 0.21 | 0.90 | 0.00 | 0.27 | 0.644 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

With oversampling:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Training | Testing | | | | | | | | | | |
| Model | Accuracy | Accuracy | Precision | | | Recall | | | F-Score | | | AUC |
| C1 | C2 | C3 | C1 | C2 | C3 | C1 | C2 | C3 |
| Log Reg | 0.5133 | 0.624 | 0.94 | 0.03 | 0.36 | 0.64 | 0.31 | 0.58 | 0.78 | 0.06 | 0.44 | 0.757 |
| DT | 0.9977 | 0.737 | 0.86 | 0.03 | 0.28 | 0.83 | 0.05 | 0.32 | 0.85 | 0.04 | 0.30 | 0.564 |
| RF | 0.9977 | 0.8117 | 0.87 | 0.00 | 0.42 | 0.92 | 0.00 | 0.33 | 0.89 | 0.00 | 0.37 | 0.722 |
| KNN | 0.9085 | 0.6367 | 0.90 | 0.03 | 0.27 | 0.67 | 0.12 | 0.54 | 0.77 | 0.05 | 0.36 | 0.637 |

1.Based on the results above; logistic Regression had high testing accuracy and precision in c1 but c2 was a complete disaster, c3 wasn’t that bad as for the results after applying oversampling training and testing dropped but we notice an improvement in c2 as the recall increased.

2. DT (Before oversampling) Training acc was high maybe caused by overfitting, testing was lower and c2 was yet again very poor; (after oversampling) testing accuracy was slightly improved and recall improved a little in c2 same as LogReg.

3. RF(Before oversampling): high training acc, but better performance in testing compared to DT,yet struggle in c2; (after oversampling): slight decrease with testing accuracy but better recall for c2 and increase in AUC means better ability to tell apart classes after oversampling.

4. KNN(Before oversampling): Lowest training acc compared to the other models, could mean less overfitting, still some weakness in c2; (after oversampling): Testing acc drops but recall in c2.

Oversampling improves recall for poorly represented classes at cost of accuracy, precision in other classes.

Some overfitting indications regarding the models before oversampling.

Oversampling helped models to identify less frequent classes better, It’s a tradeoff at the end of the day and depends on the Outcomes you’re looking for as a user and the problems you’re designing the models for.