Machine learning and Cybersecurity: Challenges, and Solutions in a Hyper-Digital Post-Pandemic Society

By

Dr. ARINDAM SARKAR

Ex. INSPIRE FELLOW, DST, Govt. of India, New Delhi

Asst. Professor, Dept. of Computer Science and Electronics,

RAMAKRISHNA MISSION VIDYAMANDIRA

(A Residential Autonomous College under University of Calcutta with CPE status)

• Belur Math • Howrah • West Bengal • Pin - 711 202 •

Class - 09

All About Confusion Matrix

- Confusion Matrix
- Accuracy
- Precision
- Recall
- F1 Measure
- Harmonic Mean
- Specificity
- Sensitivity
- AUC Curve
- ROC Curve

All About Confusion Matrix

		Prediction	
		1	0
Actual Output	1	True Positive (TP)	False Negative (FN)
	0	False Positive (FP)	True Negative (TN)

True positive (TP).

- Equivalent with hit.

True negative (TN).

- Equivalent with correct rejection.

False positive (FP).

- Equivalent with false alarm, type I error or underestimation.

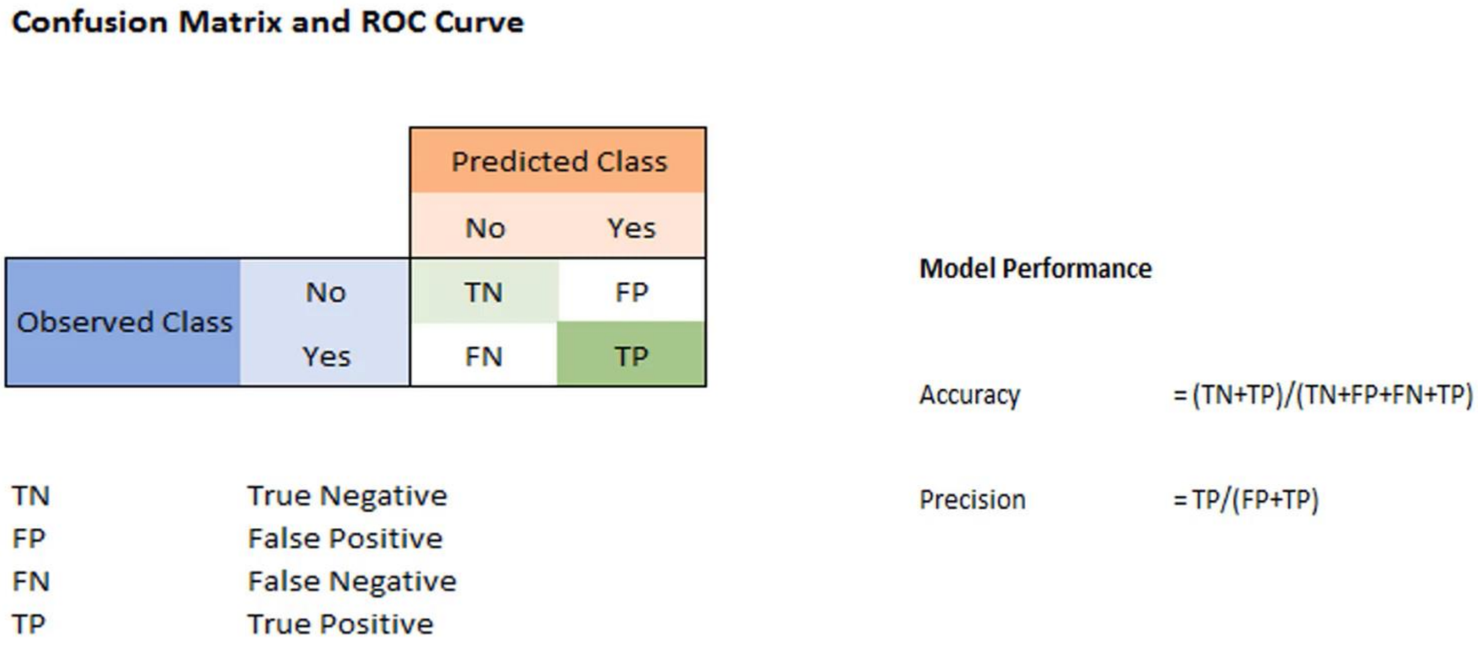
False negative (FN) .

- Equivalent with miss, type II error or overestimation.

All About Confusion Matrix

		Actual	
		Positive	Negative
Predicted	Positive	**True Positive** Predicted has cancer Has Cancer	**False Positive** Predicted has cancer/Does not have cancer
	Negative	**False Negative** Predicted not cancer Has cancer	**True Negative** Predicted not cancer Does not have cancer

Confusion Matrix



Confusion Matrix and ROC Curve

		Predicted Class	
		No	Yes
Observed Class	No	TN	FP
	Yes	FN	TP

TN	True Negative
FP	False Positive
FN	False Negative
TP	True Positive

Model Performance

Accuracy	= (TN+TP)/(TN+FP+FN+TP)
Precision	= TP/(FP+TP)

Confusion Matrix

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 = 2 \cdot \frac{precision \cdot recall}{precision + recall}$$

TP = True positive

TN = True negative

FP = False positive

FN = False negative

Accuracy

- Accuracy = (TP + TN) / (TP + FP + TN + FN)

- Condition positive (P).
  - The number of real positive cases in the data.
- Condition negative (N).
  - The number of real negative cases in the data.

Precision or Positive Predictive Value (PPV)

PPV = True Positive / (True Positive + False Positive)

All About Confusion Matrix

Sensitivity, Recall, Hit Rate, or True Positive Rate (TPR)

TPR = True Positive / (True Positive + False Negative)

All About Confusion Matrix

False Positive Rate (FPR)

$$\mathrm{FPR} = \mathrm{FP} / (\mathrm{FP} + \mathrm{TN})$$

All About Confusion Matrix

F1 Measure

F1 Measure = (Precision + Recall) / 2

All About Confusion Matrix

Harmonic Mean, F1 Score

F1 = (2 * Precision * Recall) / (Precision + Recall)

Specificity, Selectivity or True Negative Rate (TNR)

Specificity = True Negative / (True Negative + False Positive)

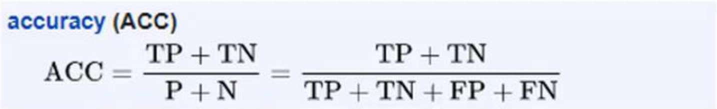
Threat Score (TS) or Critical Success Index (CSI)

CSI = TP / (TP + FN + FP)

False Discovery Rate (FDR)

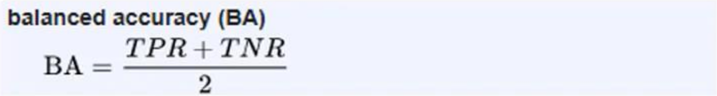
FDR = FP / (TP + FP)

All About Confusion Matrix



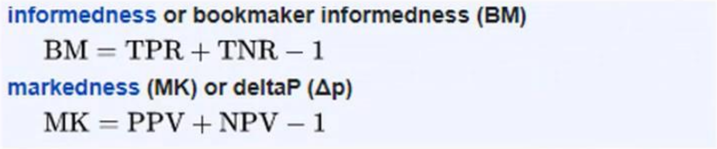
accuracy (ACC)

$$\mathrm{ACC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{P} + \mathrm{N}} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}$$



balanced accuracy (BA)

$$\mathrm{BA} = \frac{TPR + TNR}{2}$$

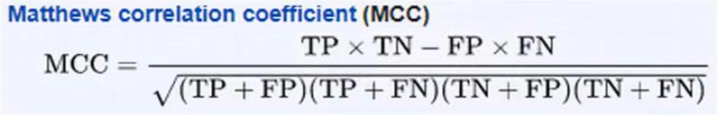


informedness or bookmaker informedness (BM)

$$\mathrm{BM} = \mathrm{TPR} + \mathrm{TNR} - 1$$

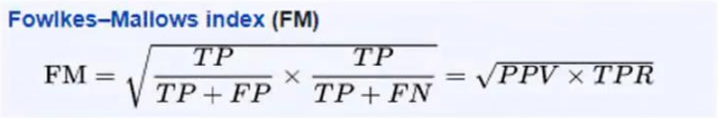
markedness (MK) or deltaP (Δp)

$$\mathrm{MK} = \mathrm{PPV} + \mathrm{NPV} - 1$$



Matthews correlation coefficient (MCC)

$$\mathrm{MCC} = \frac{\mathrm{TP} \times \mathrm{TN} - \mathrm{FP} \times \mathrm{FN}}{\sqrt{(\mathrm{TP} + \mathrm{FP})(\mathrm{TP} + \mathrm{FN})(\mathrm{TN} + \mathrm{FP})(\mathrm{TN} + \mathrm{FN})}}$$



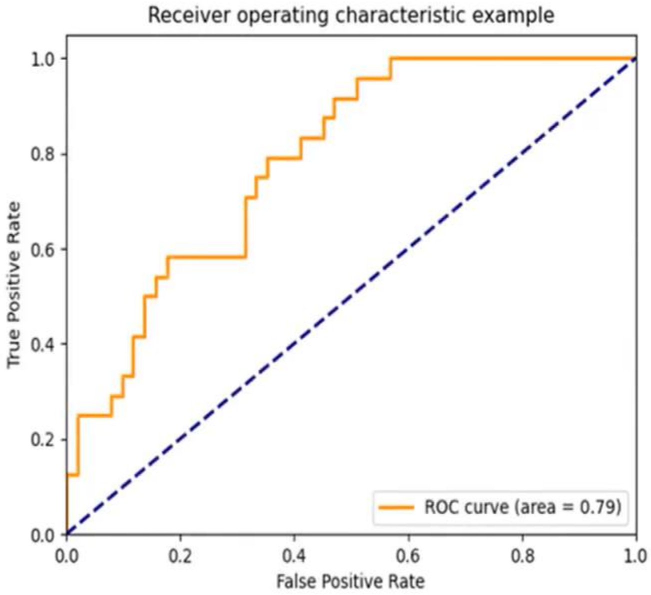
Fowlkes–Mallows index (FM)

$$\mathrm{FM} = \sqrt{\frac{TP}{TP + FP} \times \frac{TP}{TP + FN}} = \sqrt{PPV \times TPR}$$

Image: WikiPedia

ROC & AUC Curve

Receiver Operating Characteristic (ROC): Since, TPR is equivalent to Sensitivity and FPR is equal to 1 – specificity, the ROC graph is sometimes called the sensitivity vs (1 – specificity) plot.



All About Confusion Matrix

ROC & AUC Curve

Actual Result	Predicted Result
Yes	0.89
Yes	0.57
No	0.51
No	0.25
Yes	0.69
Yes	0.58

Sensitivity,
TPR = TP / (TP + FN), and

FPR = FP / (FP + TN)

Threshold Value = [0. 0.10, 0.20, 0.30, 0.40, 0.50, 0.60, 0.70

All About Confusion Matrix

ROC & AUC Curve

Actual Result	Predicted Result	Predicted (0)
Yes	0.89	1
Yes	0.57	1
No	0.51	1
No	0.25	1
Yes	0.69	1
Yes	0.58	1

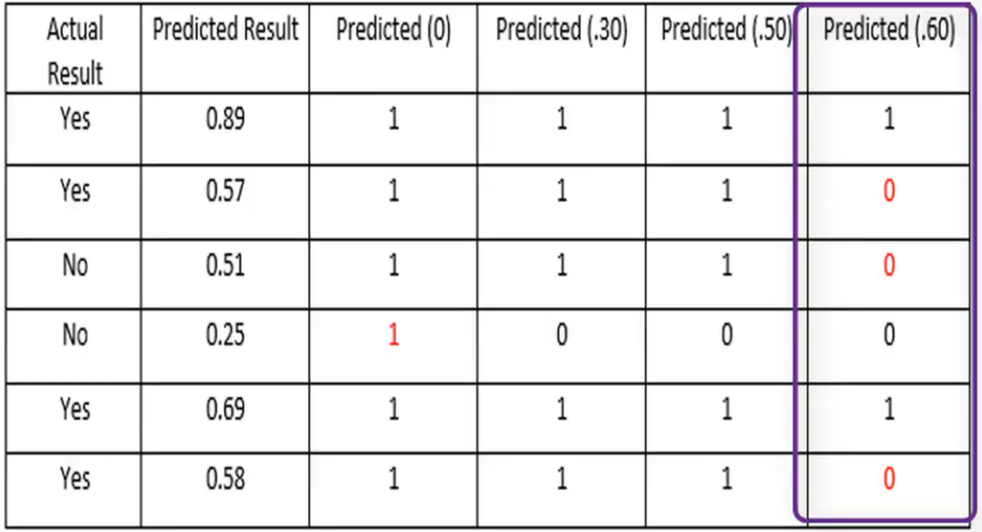
Sensitivity,
TPR = TP / (TP + FN), and

FPR = FP / (FP + TN)

Threshold Value = 0

All About Confusion Matrix

ROC & AUC Curve



Actual Result	Predicted Result	Predicted (0)	Predicted (.30)	Predicted (.50)	Predicted (.60)
Yes	0.89	1	1	1	1
Yes	0.57	1	1	1	0
No	0.51	1	1	1	0
No	0.25	1	0	0	0
Yes	0.69	1	1	1	1
Yes	0.58	1	1	1	0

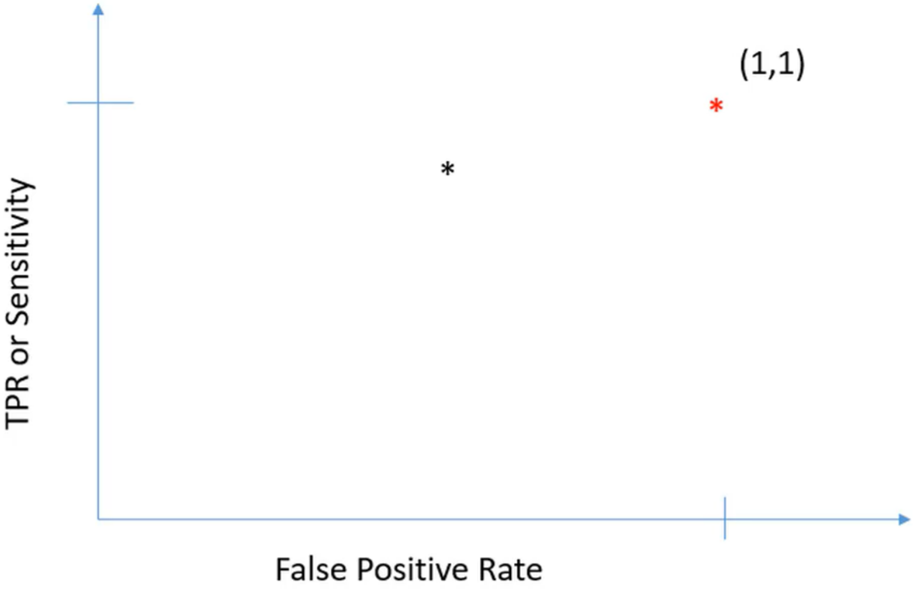
Sensitivity,
TPR = TP / (TP + FN), and

FPR = FP / (FP + TN)

Threshold Value = 0.60

All About Confusion Matrix

ROC & AUC Curve



Actual Result	Predicted Result	Predicted (0)
Yes	0.89	1
Yes	0.57	1
No	0.51	1
No	0.25	1
Yes	0.69	1
Yes	0.58	1

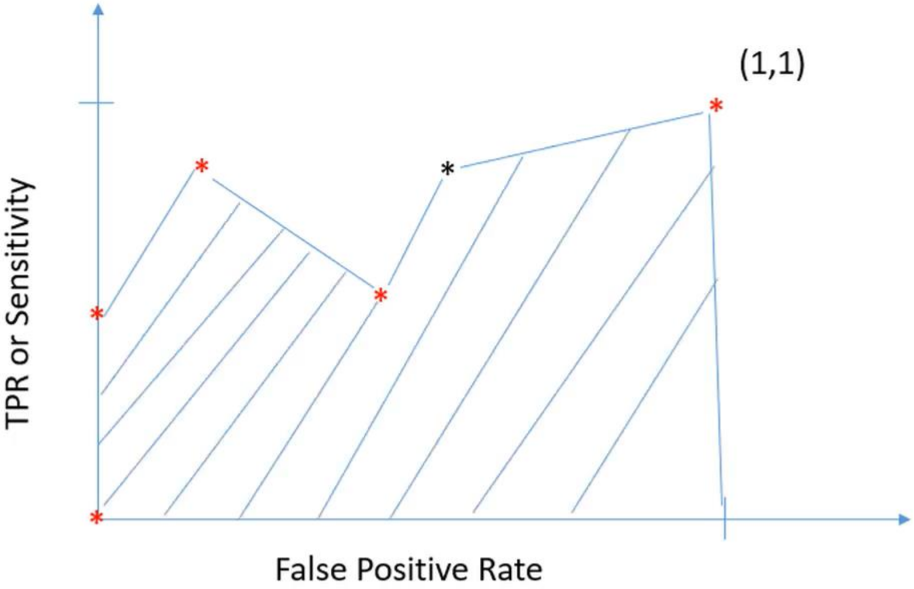
Sensitivity,

$$\begin{aligned} TPR &= TP \,/\, (TP + FN) \\ &= 4 \,/\, 4 + 1 \\ &= .80 \end{aligned}$$

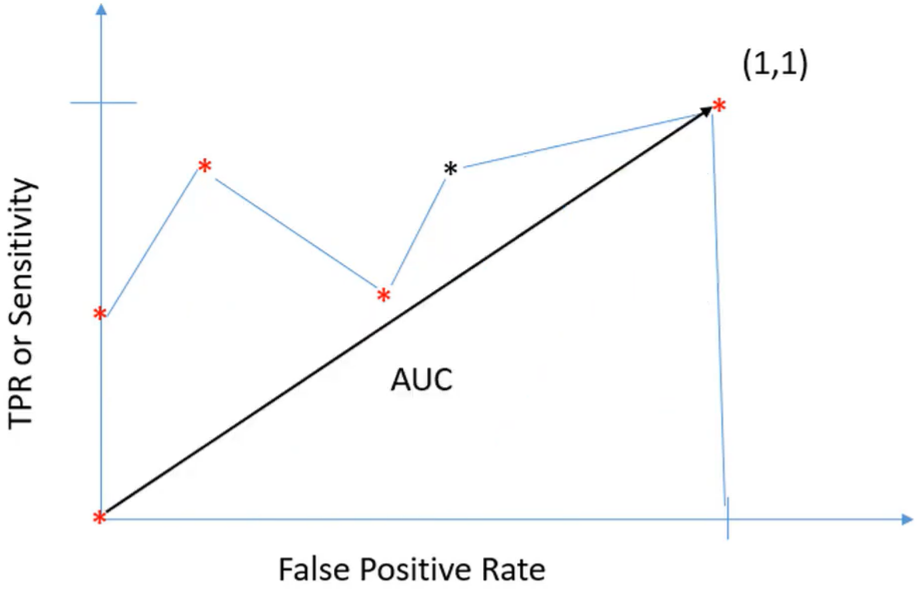
$$\begin{aligned} FPR &= FP \,/\, (FP + TN) \\ &= 1 \,/\, 1 + 1 \\ &= 0.5 \end{aligned}$$

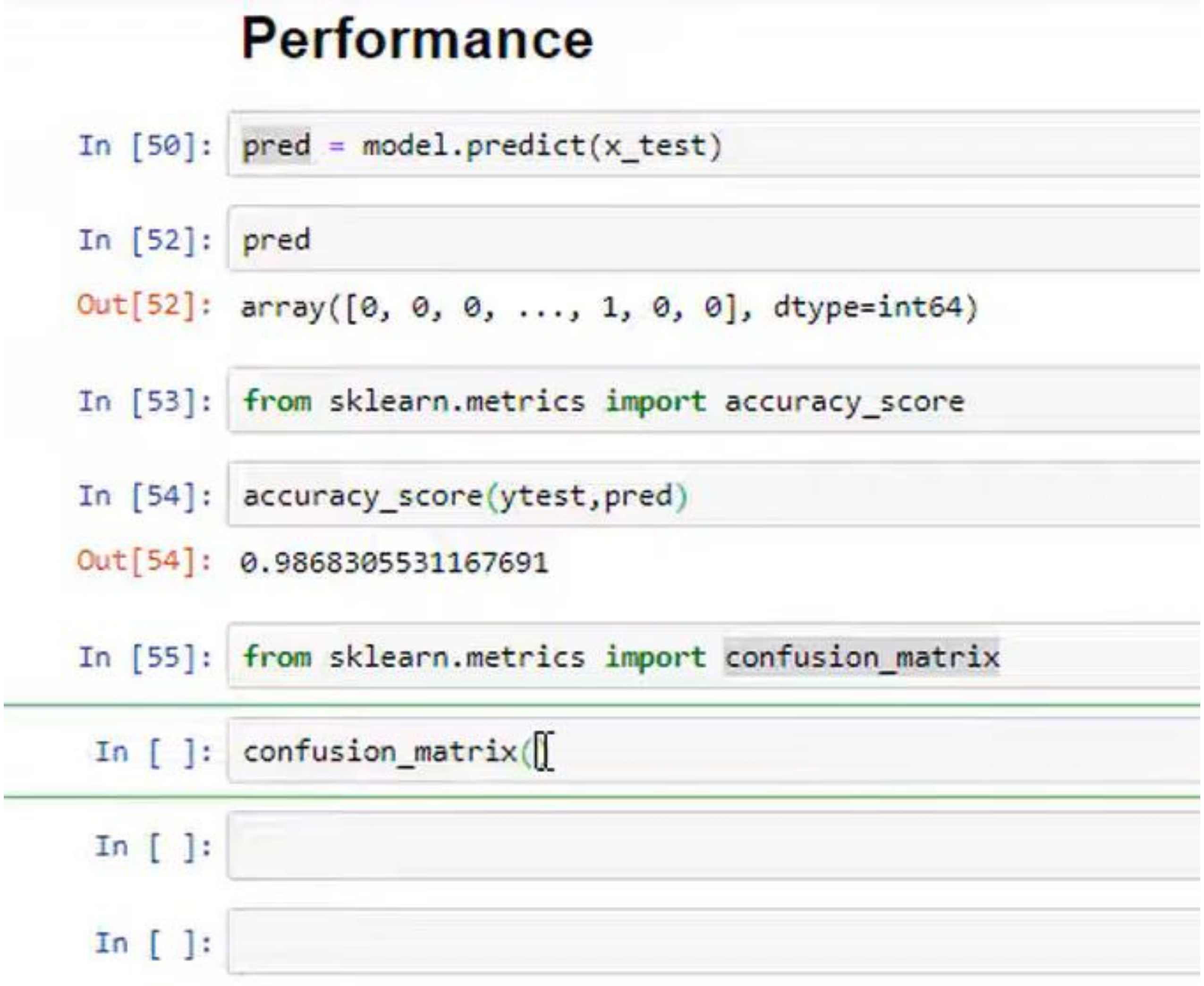
All About Confusion Matrix

ROC & AUC Curve



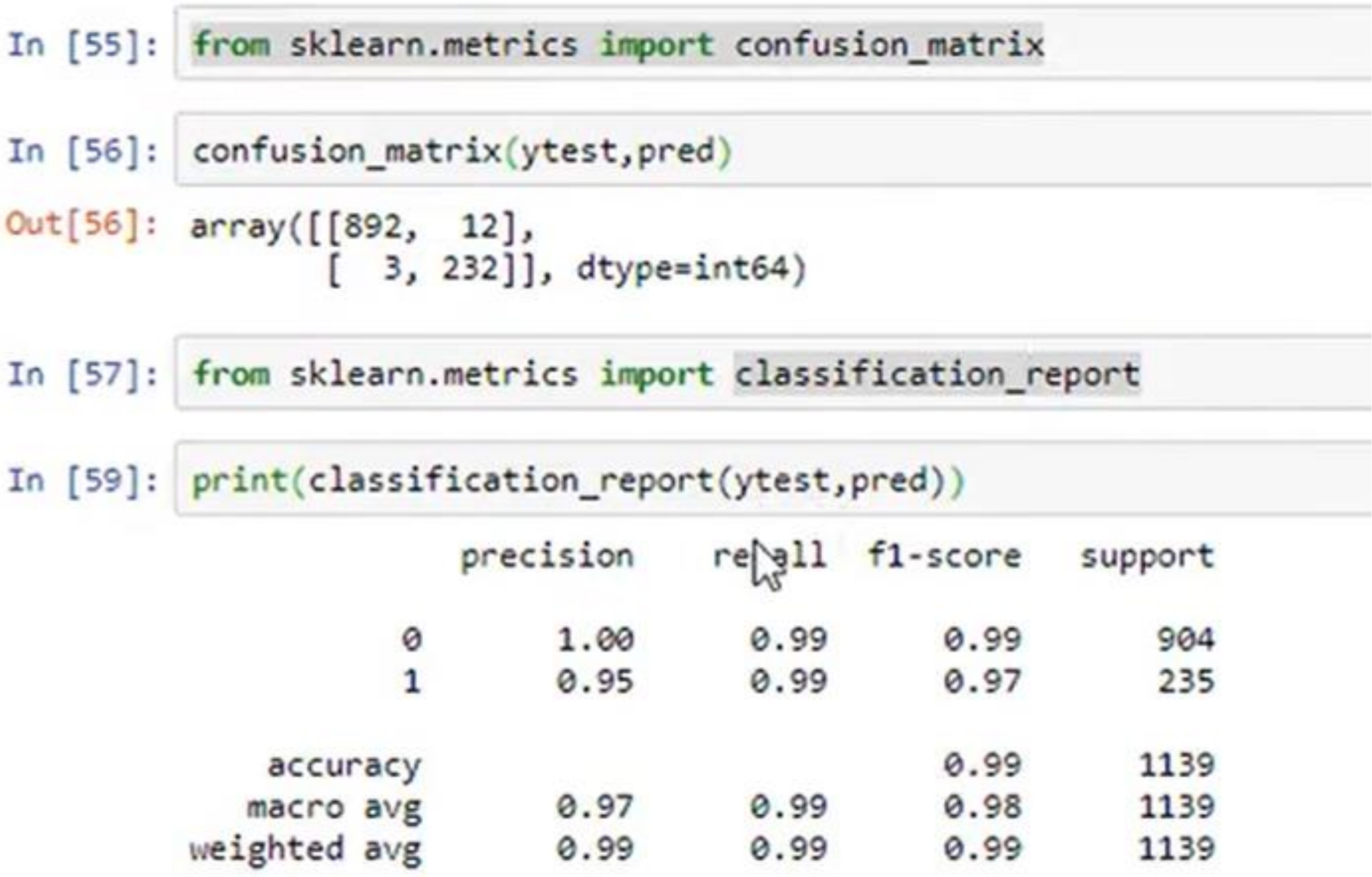
ROC & AUC Curve





Performance

```
In [50]: pred = model.predict(x_test)

In [52]: pred

Out[52]: array([0, 0, 0, ..., 1, 0, 0], dtype=int64)

In [53]: from sklearn.metrics import accuracy_score

In [54]: accuracy_score(ytest,pred)

Out[54]: 0.9868305531167691

In [55]: from sklearn.metrics import confusion_matrix

In [ ]: confusion_matrix()

In [ ]:

In [ ]:
```



```
In [55]: from sklearn.metrics import confusion_matrix

In [56]: confusion_matrix(ytest,pred)

Out[56]: array([[892,  12],
                [  3, 232]], dtype=int64)

In [57]: from sklearn.metrics import classification_report

In [59]: print(classification_report(ytest,pred))

              precision    recall  f1-score   support

           0       1.00      0.99      0.99       904
           1       0.95      0.99      0.97       235

    accuracy                           0.99      1139
   macro avg       0.97      0.99      0.98      1139
weighted avg       0.99      0.99      0.99      1139
```

Thank You