Evaluation of Machine Learning Algorithms for Anomaly Detection

Nebrase Elmrabit - Department of Cyber Security Glasgow Caledonian University, UK

Huiyu Zhou and Feixiang Zhou - School of Informatics University of Leicester, UK

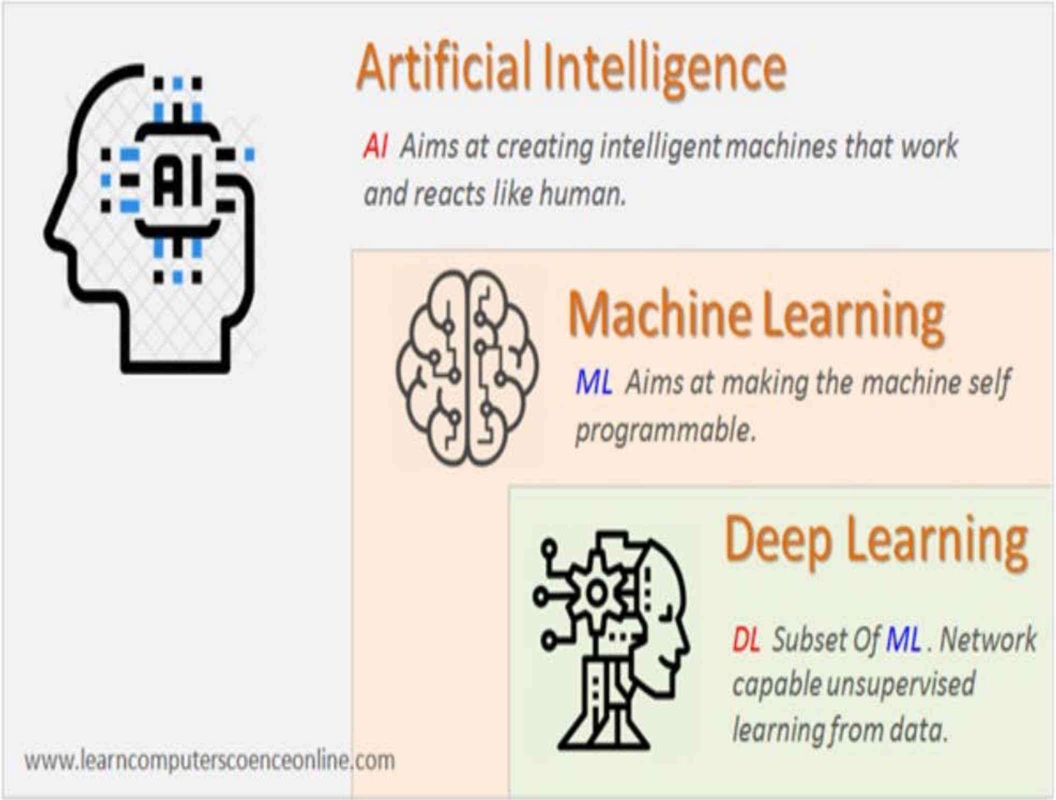
Fengyin Li - School of Information Science Qufu Normal University, China

Outlines

- Introduction
- Background
- Methodology
- Experiments
- Experimental Results
- Discussion
- Conclusion

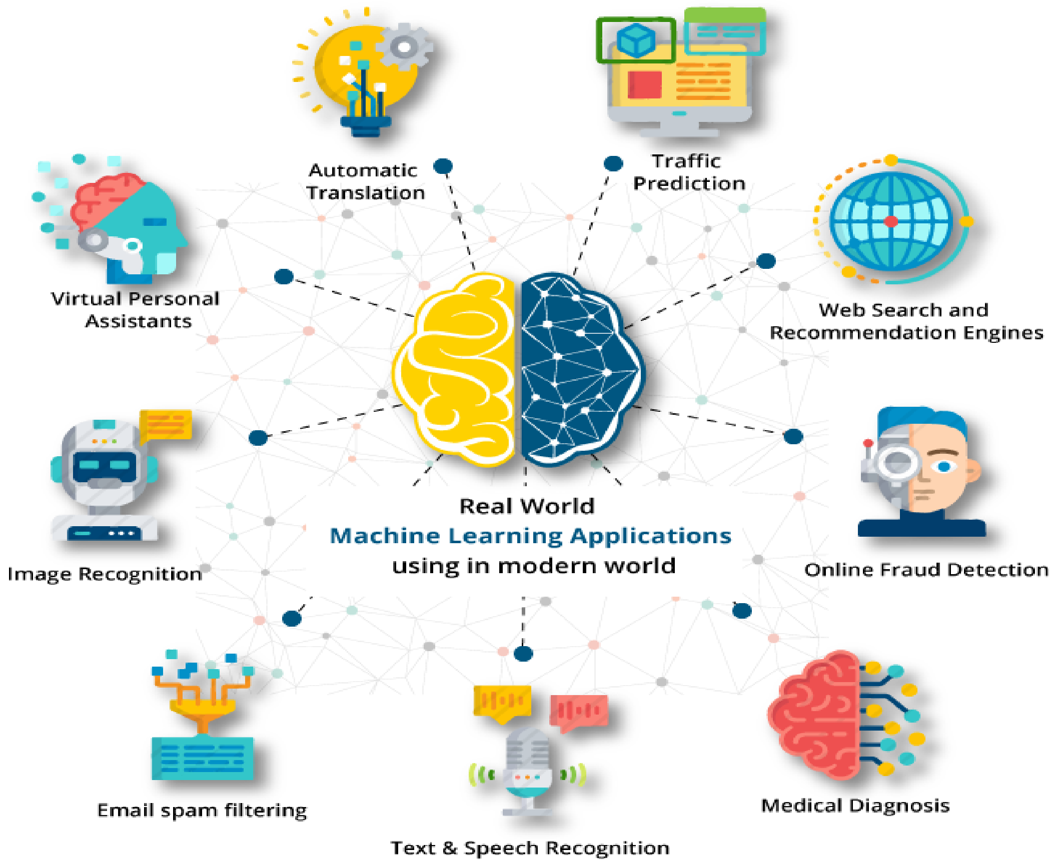
Introduction

- The challenge of anomaly detection in the context of cyber-security:-
  - Motivation, Opportunity and Capability
  - Attacks
- Signature-based approaches
  - Zero-day attacks
  - Encrypted traffic
- Artificial Intelligence (AI) technologies
  - Predicting the anomaly behaviours of malicious attacks
  - Classify data collected into
  - Maintaining a low false alarm rate



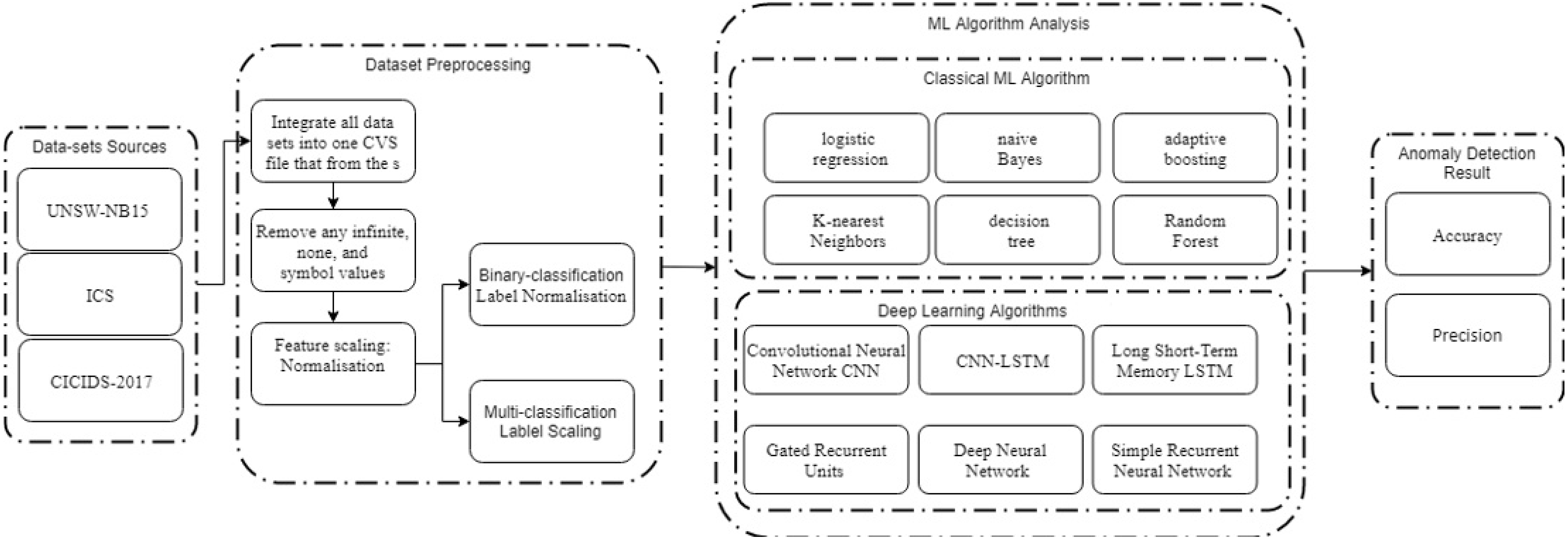
Background

- Applications of ML Algorithms.
  - Problem-solving approach
  - Multidisciplinary
- ML in cyber-security field.
  - Prediction, prevention, detection, response, and monitoring.
- The current implementation challenges.
  - Accuracy
  - Cost
  - Policies etc.



https://www.learncomputerscienceonline.com/what-is-machine-learning/

Methodology



Experiments

- Experimental Environment
  - High performance computing facility at the University of Leicester
  - Python-3.6.8
  - Scikit-learn-0.21.3 ML library
  - Keras-2.3.04 neural-network library and Tensor-Flow-1.9.05
  - Sigmoid and SoftMax functions
  - Pandas6 and NumPy7 library packages

Experiments

- Data Pre-processing
  - Convert and integrate all the files from the same dataset to one single CSV file.
  - Delete any infinite, none, and symbol values.
  - Feature scaling by normalising all the features.
  - Label normalisation or scaling.
- Performance Metrics
  - Accuracy
  - Precision
  - True Positive Rate (TPR), also known as Recall
  - False Positive Rate (FPR)
  - F1-Score
  - Receiver Operating Characteristic (ROC) curve
  - Confusion Matrix

Experimental Results

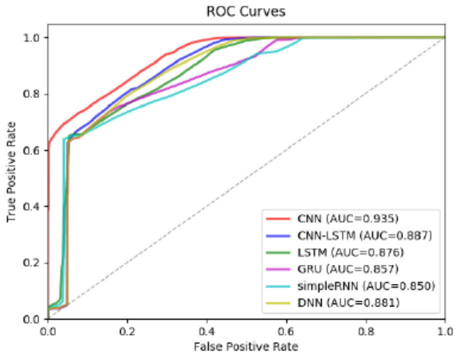
Binary Classification

Methods	Accuracy	Precision	Recall	F-score
UNSW-NB15				
LR	0.753	0.858	0.735	0.792
GNB	0.716	0.693	0.997	0.818
KNN	0.829	0.851	0.887	0.869
DT	0.885	0.914	0.906	0.910
AdaB	0.839	0.817	0.965	0.884
RF	0.877	0.844	0.991	0.912
CNN	0.856	0.825	0.983	0.897
CNN-LSTM	0.835	0.804	0.980	0.889
LSTM	0.767	0.893	0.721	0.798
GRU	0.777	0.857	0.782	0.818
SimpleRNN	0.807	0.775	0.984	0.867
DNN	0.827	0.793	0.987	0.879
CICIDS-2017				
LR	0.883	0.737	0.634	0.682
GNB	0.550	0.298	0.946	0.453
KNN	0.996	0.987	0.994	0.990
DT	0.998	0.995	0.996	0.996
AdaB	0.962	0.898	0.910	0.904
RF	0.999	0.997	0.997	0.997
CNN	0.996	0.991	0.989	0.990
CNN-LSTM	0.993	0.989	0.992	0.991
LSTM	0.994	0.967	0.961	0.964
GRU	0.994	0.981	0.989	0.989
SimpleRNN	0.983	0.965	0.951	0.958
DNN	0.991	0.976	0.987	0.981
ICS cyber-attack datasets				
LR	0.710	0.710	1.000	0.830
GNB	0.709	0.710	0.999	0.830
KNN	0.849	0.882	0.909	0.895
DT	0.864	0.905	0.903	0.904
AdaB	0.720	0.732	0.956	0.829
RF	0.928	0.929	0.972	0.950
CNN	0.715	0.715	0.999	0.834
CNN-LSTM	0.715	0.715	1.000	0.833
LSTM	0.715	0.715	1.000	0.833
GRU	0.715	0.715	1.000	0.834
SimpleRNN	0.715	0.715	0.999	0.834
DNN	0.716	0.716	1.000	0.834

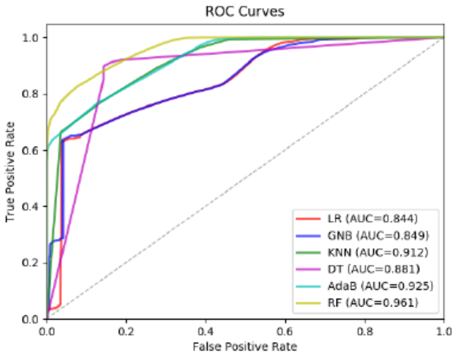
Multi-class Classification

Methods	Accuracy	Precision	Recall	F-score
UNSW-NB15				
LR	0.561	0.497	0.561	0.428
GNB	0.085	0.587	0.085	0.130
KNN	0.652	0.638	0.652	0.638
DT	0.735	0.715	0.735	0.718
AdaB	0.631	0.553	0.631	0.557
RF	0.736	0.726	0.736	0.695
CNN	0.684	0.672	0.684	0.627
CNN-LSTM	0.680	0.619	0.680	0.615
LSTM	0.661	0.601	0.661	0.598
GRU	0.665	0.600	0.661	0.608
SimpleRNN	0.662	0.585	0.662	0.587
DNN	0.663	0.664	0.663	0.608
CICIDS-2017				
LR	0.915	0.914	0.915	0.910
GNB	0.430	0.846	0.430	0.522
KNN	0.996	0.996	0.996	0.996
DT	0.998	0.998	0.998	0.998
AdaB	0.818	0.769	0.818	0.760
RF	0.999	0.999	0.999	0.999
CNN	0.997	0.996	0.997	0.996
CNN-LSTM	0.994	0.993	0.994	0.994
LSTM	0.991	0.990	0.991	0.989
GRU	0.993	0.993	0.993	0.991
SimpleRNN	0.994	0.993	0.994	0.993
DNN	0.998	0.998	0.998	0.998
ICS cyber-attack datasets				
LR	0.068	0.036	0.068	0.017
GNB	0.107	0.164	0.107	0.062
KNN	0.877	0.878	0.877	0.877
DT	0.924	0.924	0.924	0.924
AdaB	0.185	0.070	0.185	0.090
RF	0.920	0.920	0.920	0.920
CNN	0.061	0.004	0.061	0.007
CNN-LSTM	0.061	0.004	0.062	0.007
LSTM	0.369	0.307	0.369	0.319
GRU	0.321	0.240	0.321	0.262
SimpleRNN	0.244	0.189	0.244	0.198
DNN	0.379	0.332	0.379	0.308

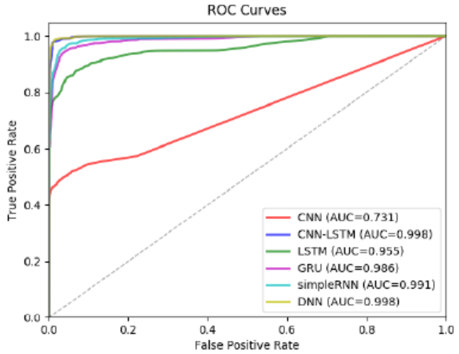
Discussion



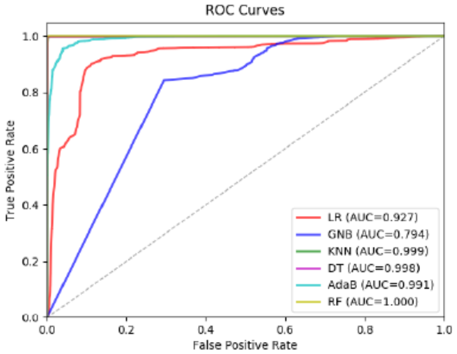
(a) Deep Learning – UNSW



(b) Classic ML – UNSW

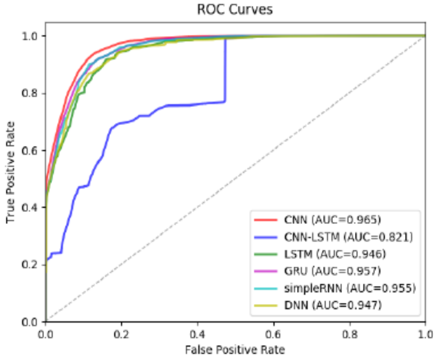


(c) Deep Learning – CICIDS

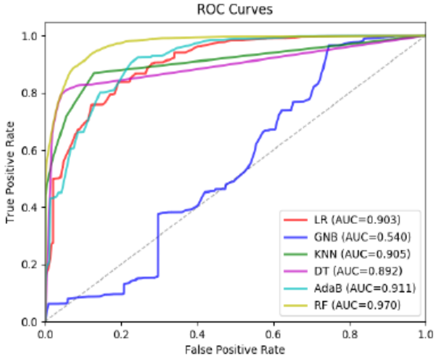


(d) Classic ML- CICIDS

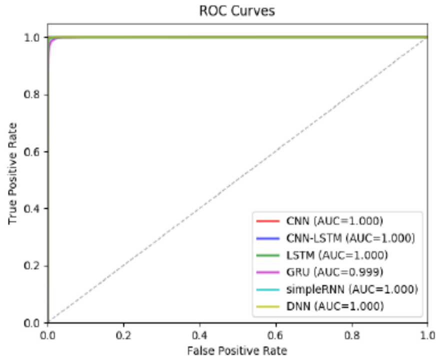
Binary Classification ROC Curves



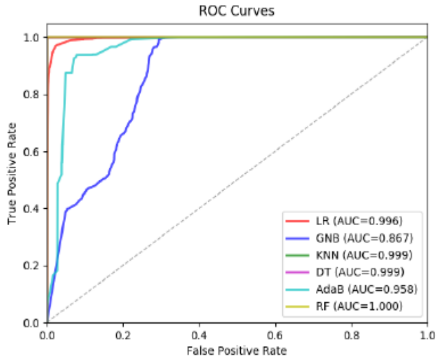
(a) Deep Learning – UNSW



(b) Classic ML – UNSW



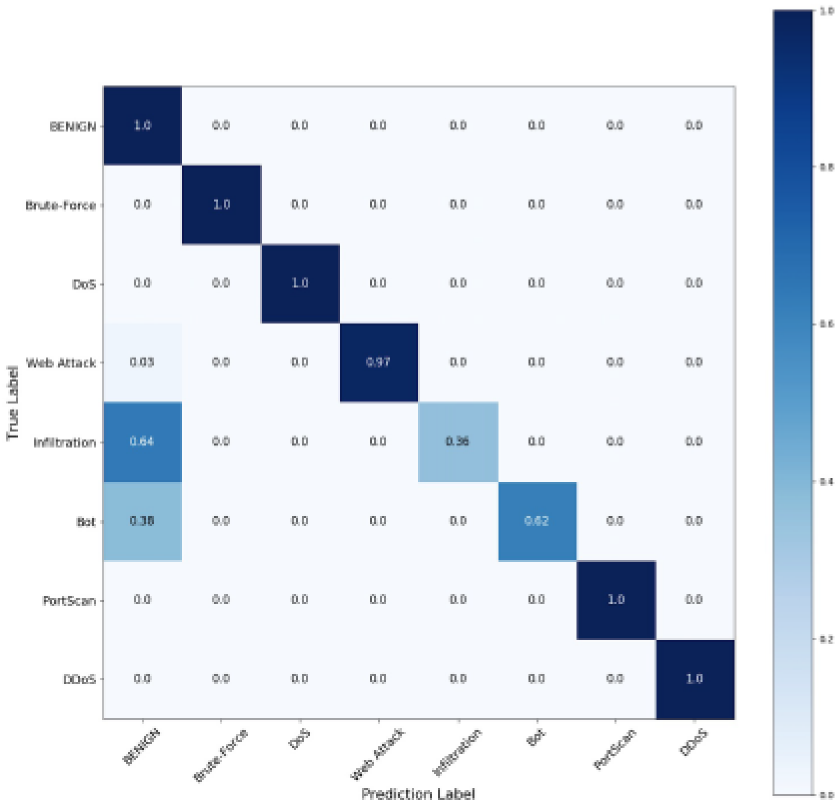
(c) Deep Learning – CICIDS



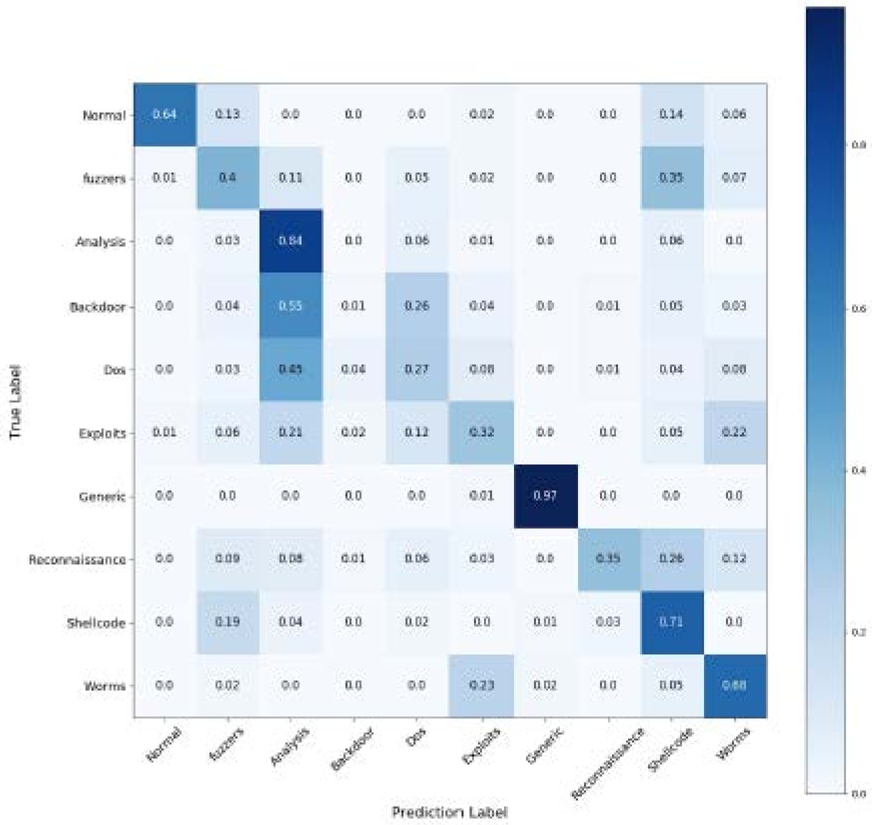
(d) Classic ML- CICIDS

Multi Classification ROC Curves

Discussion



RF Confusion Matrix Result for CICIDS-2017 Dataset.



RF Confusion Matrix Result for UNSW-NB15 Dataset.

Conclusion

- Evaluated the performance of the twelve ML algorithms.
- Recommend the best-fit algorithms
- Identified the lowest performance algorithms.
- Next step

Thanks

Nebrase Elmrabit
Department of Cyber Security
Glasgow Caledonian University
Glasgow, UK
nebrase.elmrabit@gcu.ac.uk

Feixiang Zhou
School of Informatics
University of Leicester
Leicester, UK
fz64@leicester.ac.uk

Fengyin Li
School of Information Science
Qufu Normal University
Rizhao 276826, China
lfyin318@126.com

Huiyu Zhou
School of Informatics
University of Leicester
Leicester, UK
hz143@leicester.ac.uk