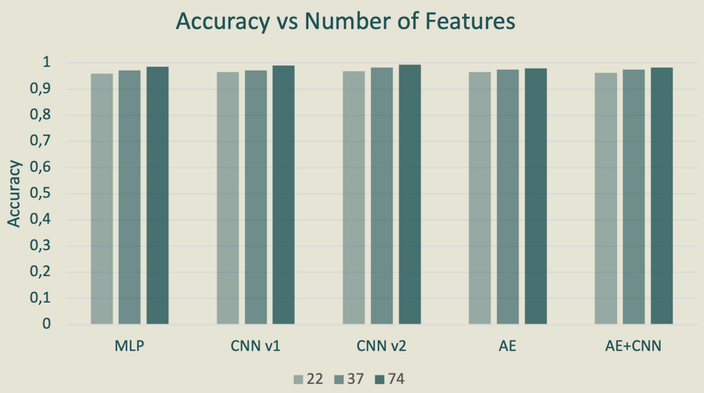
# Deep Learning for Malware Detection

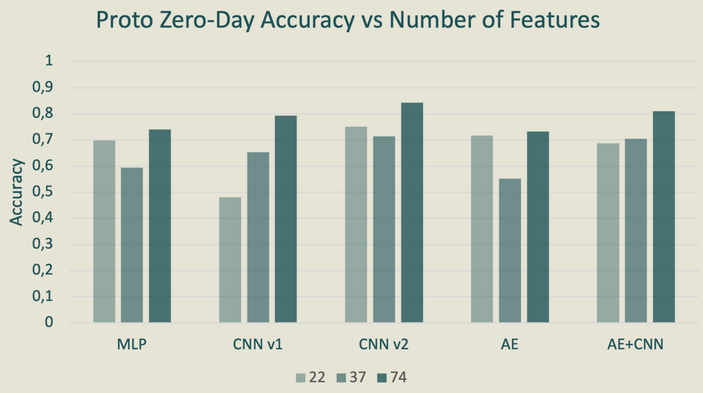
**Malware Detection** is the process of identifying malicious software within a network, aiming to maintain the integrity, confidentiality, and availability of information. Deep Learning offers an approach which does not face the same limitations as classical detection systems. DL4MD presents an evaluation of deep learning models when tasked with detecting botnet and ransomware traffic.

## Botnet Detection

When we reduce the feature space in botnet detection models, we observed a noticeable decline in their ability to accurately classify malware. Although these models perform well when tasked with identifying known malware, they faced challenges in a proto zero-day testing environment, which is designed to simulate attacks from yet-to-be-discovered or unknown malware types. Among all the models we tested, the deep Convolutional Neural Network (CNN) was the most effective in terms of its ability to generalize to these unknown botnets.

While we found that a reduction in feature space had an associated decline in memory usage, there was no apparent effect on inference time.



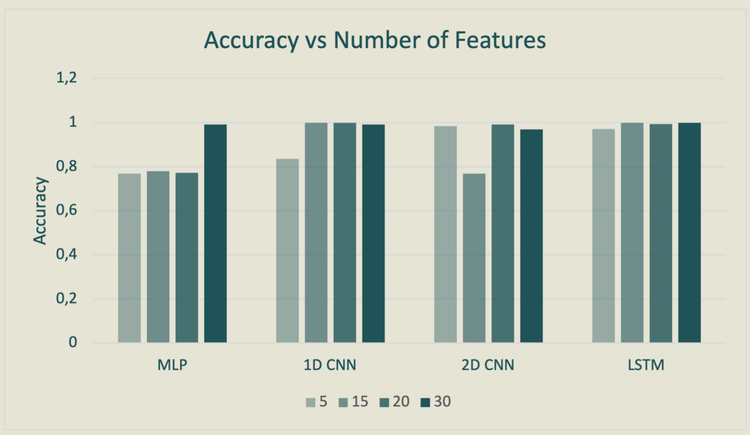

| Model | Memory Use (mb) | | | Inference Time (ms) | | |
|---|---|---|---|---|---|---|
| Features | 23 | 37 | 74 | 23 | 37 | 74 |
| CNN v1 | 422.39 | 422.91 | 465.89 | 0.0002 | 0.0002 | 0.0003 |
| CNN v2 | 435.83 | 443.78 | 526.16 | 0.0002 | 0.0002 | 0.0003 |
| AE | 457.02 | 428.02 | 457.02 | 0.0002 | 0.0002 | 0.0002 |
| AE+CNN | 475.42 | 485.50 | 490.94 | 0.0003 | 0.0002 | 0.0002 |
| MLP | 416.67 | 422.70 | 446.05 | 0.0002 | 0.0002 | 0.0002 |

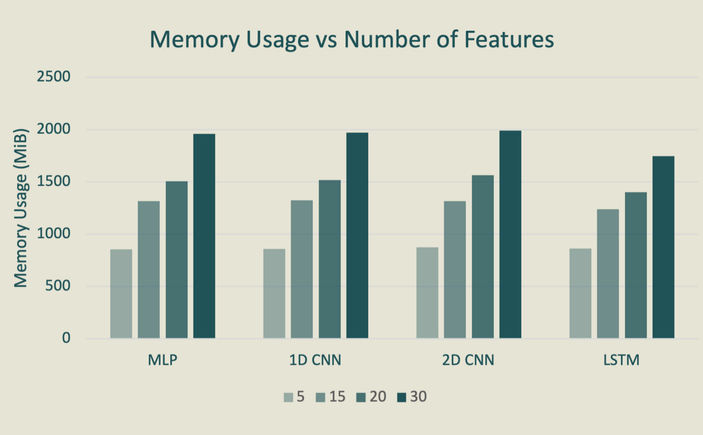
## Ransomware Detection

The LSTM model performs consistently well across all input sizes (5, 15, 20, 30). Increasing the amount of features used does not result in increased accuracy.

An increased number of features inputted into the model results in increased memory usage. The LSTM model achieves the lowest memory usage overall.

There is no universally perfect model, and a model selection should be tailored to the needs of the network.




| Model | False Positives | False Negatives | Inference Time (ms) |
|---|---|---|---|
| MLP | 629 | 229 | 23 |
| 1D CNN | 2 | 48 | 34 |
| 2D CNN | 0 | 11353 | 37 |
| LSTM | 530 | 19 | 89 |
| Window LSTM | 1054 | 75 | 26 |

## Conclusions

Our findings indicate that Deep Learning models are capable of detecting malware to an acceptible degree of accuracy. Moreover, we observed larger feature spaces being associated with increased memory utilisation and better classification performance. This highlights the need for more careful feature selection for less complex datasets which are yield the same classification performance. Finally, we recognise promising proof of concept that malware classifiers are able to generalise from their training data to entirely unknown malware famiilies.

**University of Cape Town**
Department of Computer Science
*www.sit.uct.ac.za*

**Supervisors**
Dr. Josiah Chavula
Prof. Geoff Nitschke

**Authors**
Lucas Carr
Cristopher Lamprecht