PRESENTED BY GROUP 24

EXAMINING ANOMALY DETECTION AND REINFORCEMENT LEARNING TECHNIQUES

https://redfoxsec.com/blog/top-cybersecurity-trends-2023/

CMPT 318 TERM PROJECT

FALL 2023

Submitted By: Rebecca Reedel (301454910), Asmita Srivastava (301436340), Mrinal Goshalia (301478325)

INTRODUCTION

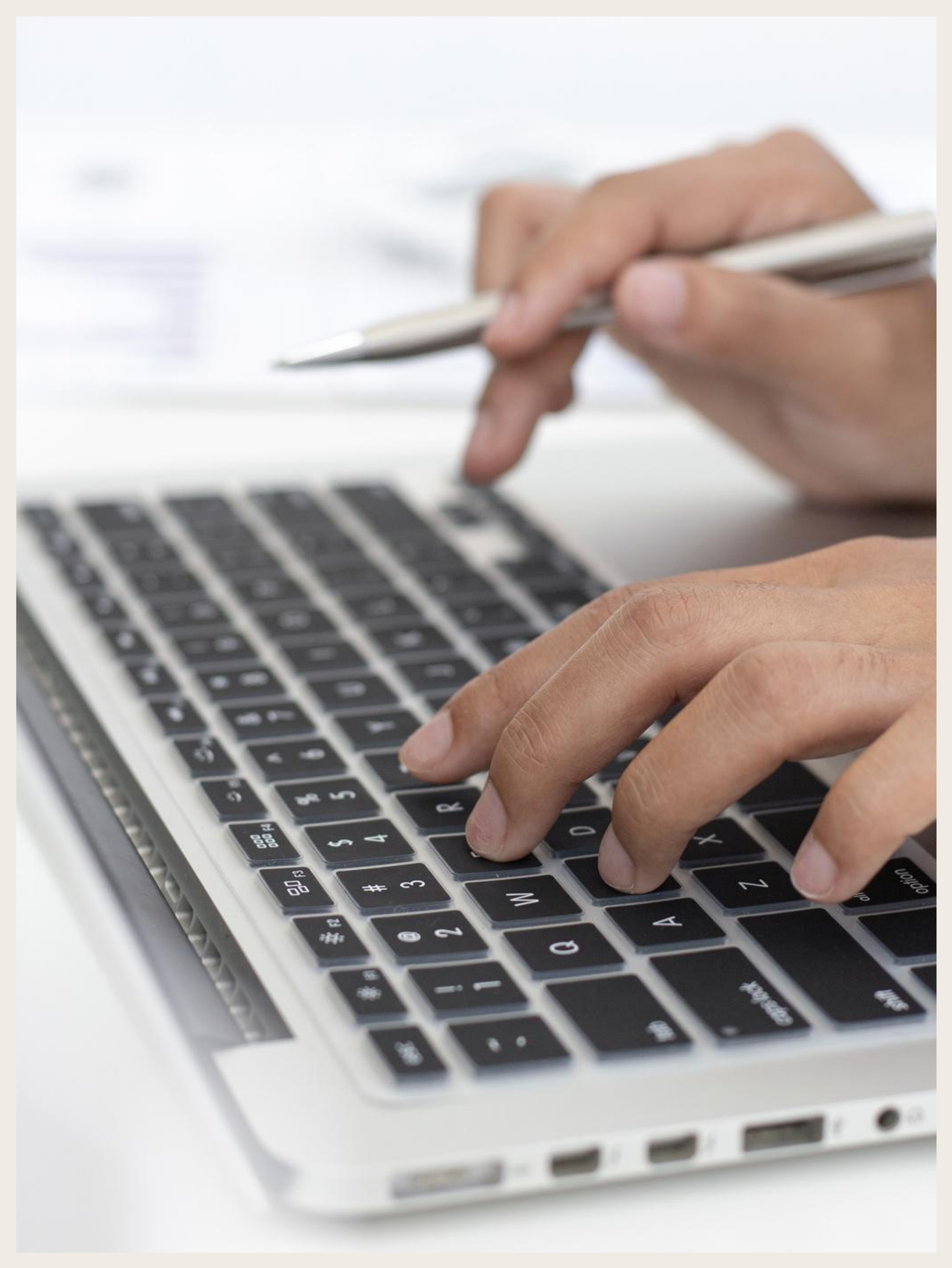
- The Cyber Threat Landscape is evolving.
- More complicated attacks require More Sophisticated Detection Systems and Mitigations.
- Zero-day Exploits are increasingly popular and are undetectable by Signature-Based IDS.

PROBLEM SCOPE

One of the many ways the Cyber Attack Space is growing, is the increasing popularity of automated systems, such as **Supervisory Control Systems**.

Malicious Attacks on SCS can cause devastating **cascading failures**.

An example would be an attack on the Electrical Grid Controls of a Hospital.



SOLUTION

Since Supervisory Control Systems automate the processes of **critical** resources, it is imperative that malicious and anomalous behaviours be **detected VERY quickly!**

Therefore, we need **automated systems** monitoring all processes. This is done through Anomalous Intrusion Detection Systems using **Machine Learning** Technology.

FEATURE ENGINEERING

Scaling Data

Standardize response variables, so within same range

PCA

Use Principal Component Analysis to eliminate redundant data

Interpret Results

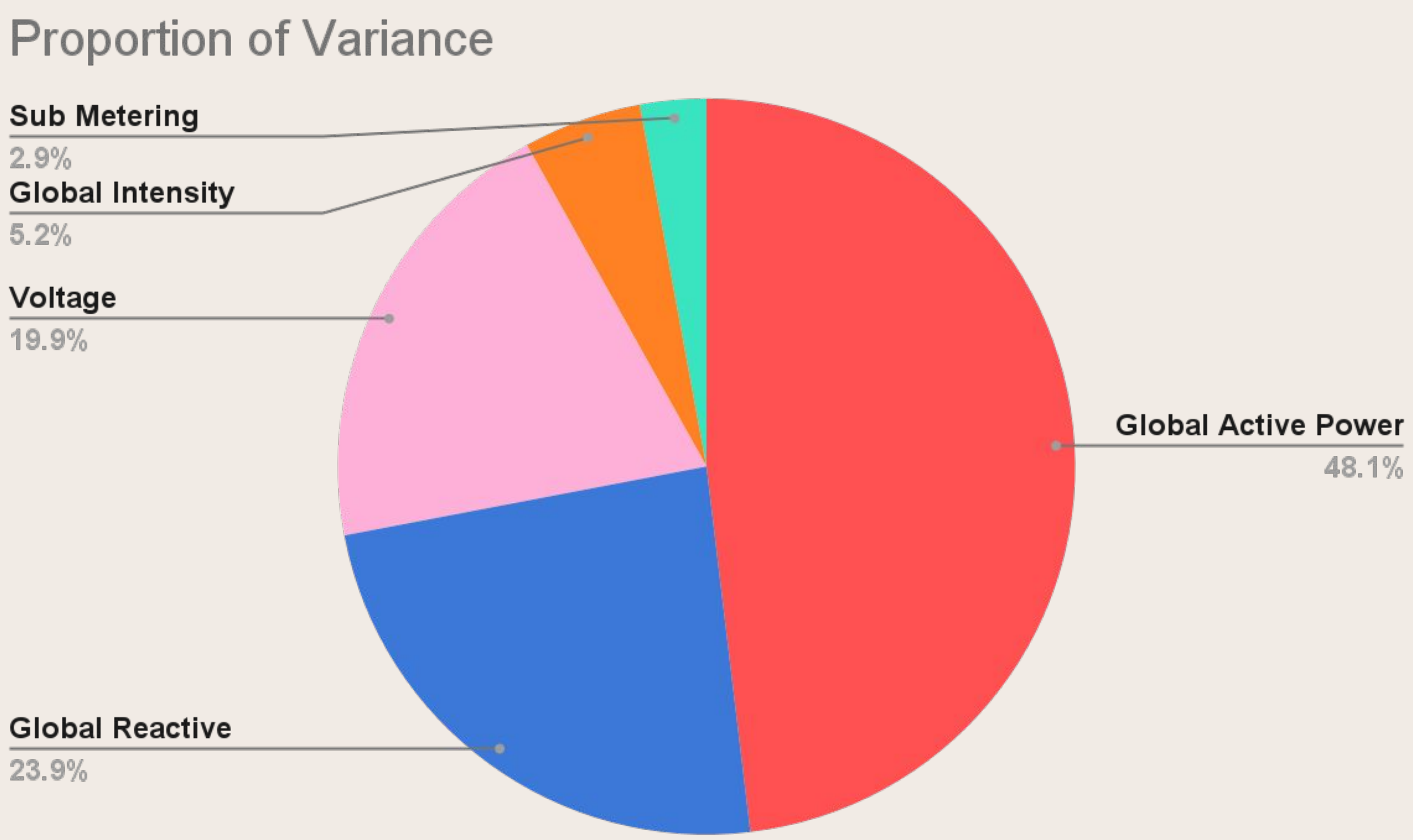
Plot and analyze principal components and evaluate response variables

Extract Features

Select subset of features determined after PCA to be used in HMMs

Principal Component Analysis

- Feature engineering technique to assess and model raw data.
- Helps in reducing redundancy from multi-dimensional data to essential components.
- Goal : Reduce redundancy in data by extracting 3 principal components on energy consumption data.



Principal Component Analysis Cont.

- Contribution by Voltage:

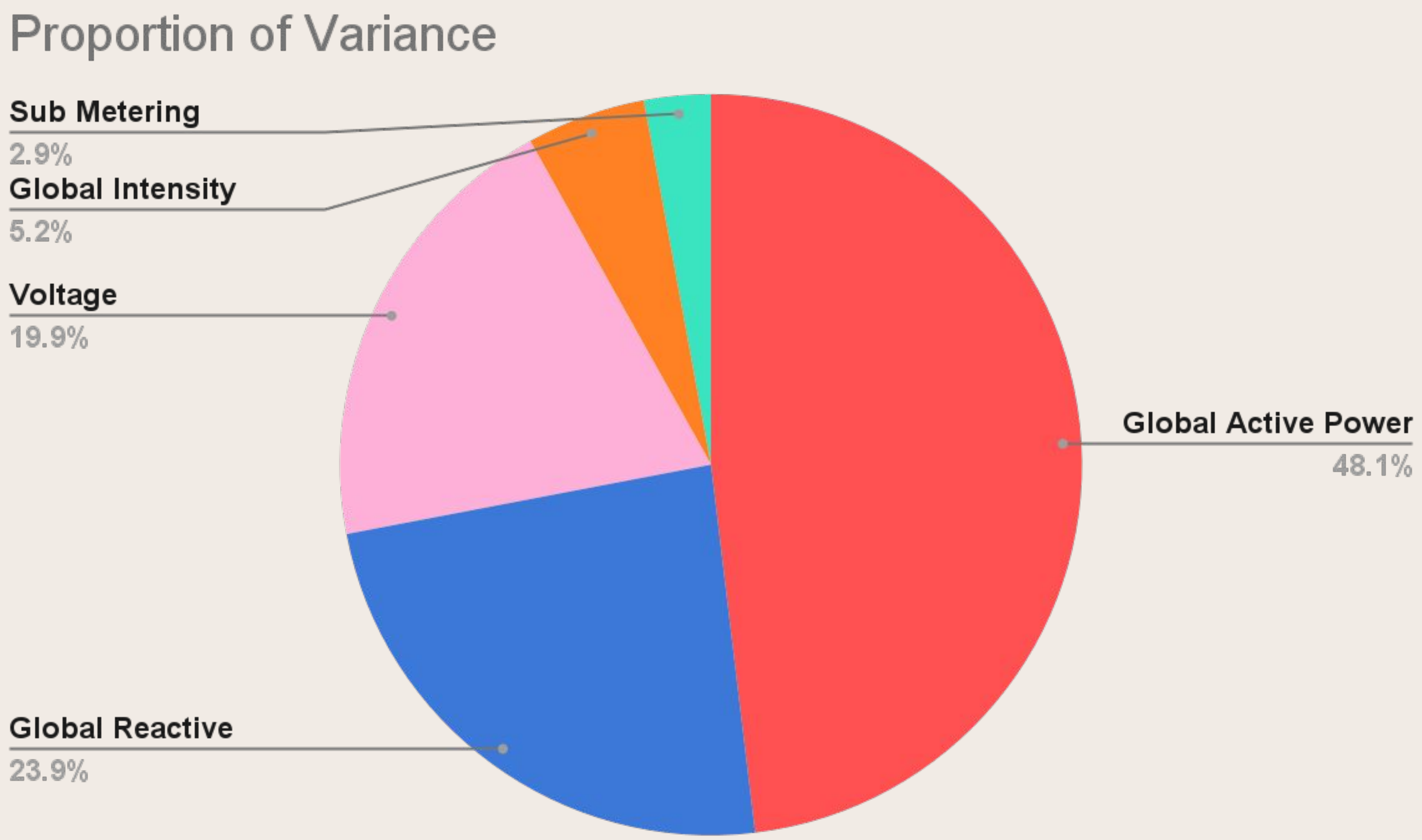
2.108480e+00*(48.1%) + 0.5697202583*(23.9%)

- Contribution by Global Intensity:

1.733467e+01*(48.1%) + 5.9705662244*(23.9%)

- Principal Components:

Global Active Power, Global Reactive Power and Global Intensity.



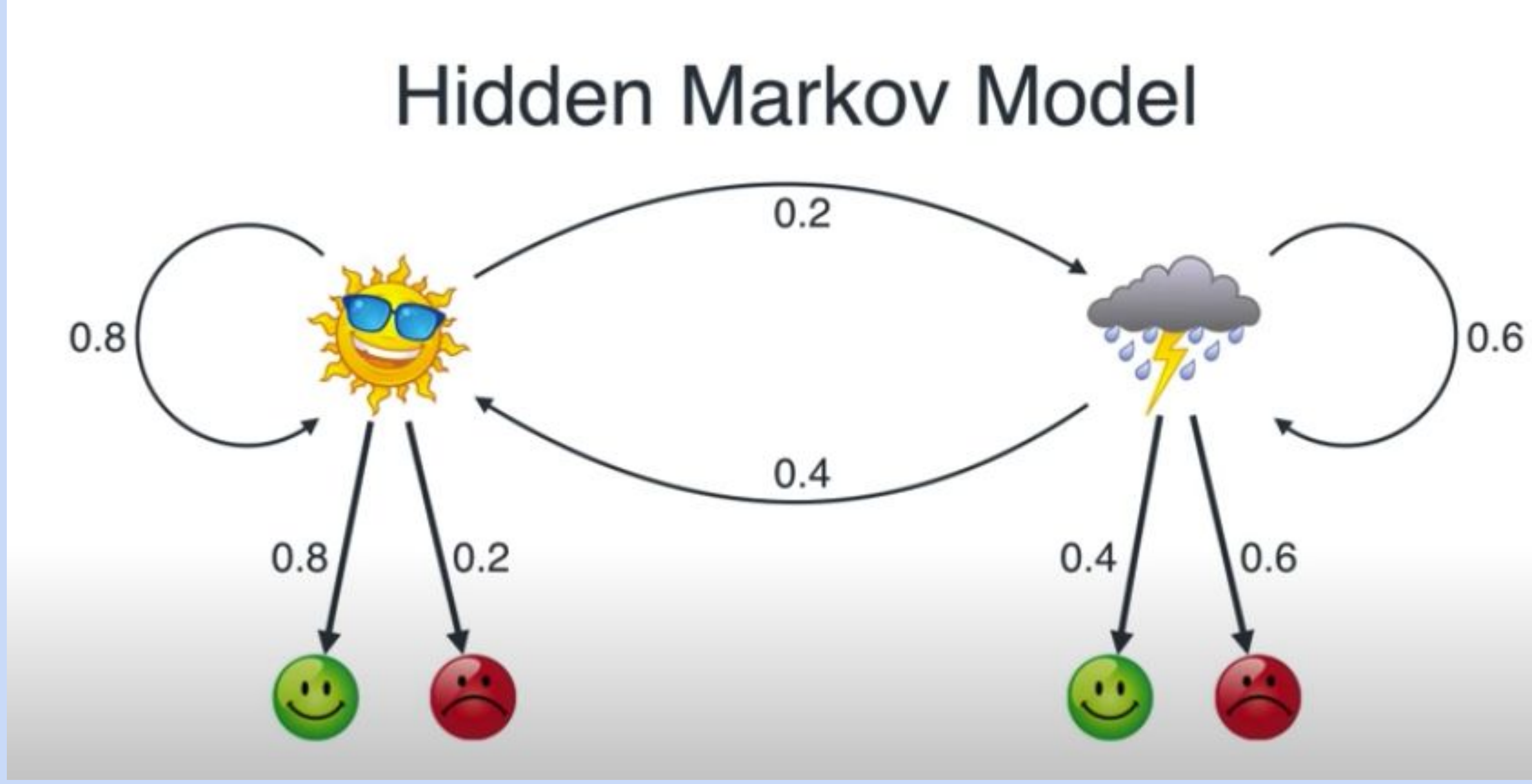
TIME WINDOW

WEDNESDAYS, 00:00:00 - 04:00:00

- The time window was selected after due diligence based on time series' dimensions.
- This time window yields = 36960 observations, which is (154 wednesdays) x (240 minutes) worth of data.

Hidden Markov Models

- HMMs are a form of probabilistic modelling, taking into account state transition and their probability of outcomes.
- The true state is 'hidden', hence needing to be estimated as different stages in the model training process.
- An HMM model involves a set of parameters which it can be modelled using, these parameters are based upon the data provided under training.
- HMMs can help predict malware if we train it under some 'normal' designated data and have it deviate from any possible security threats known as anomalies.



https://gist.github.com/fohria

TRAIN-TEST SPLIT

When creating a Hidden Markov Model, it is very important to split the initial data into **train** and **test** sets.

- **Train set**: used during creation of the HMM, and is what the model learns from.
- **Test set:** used on the model afterwards and is crucial for checking that the model will react well to **unseen data**.

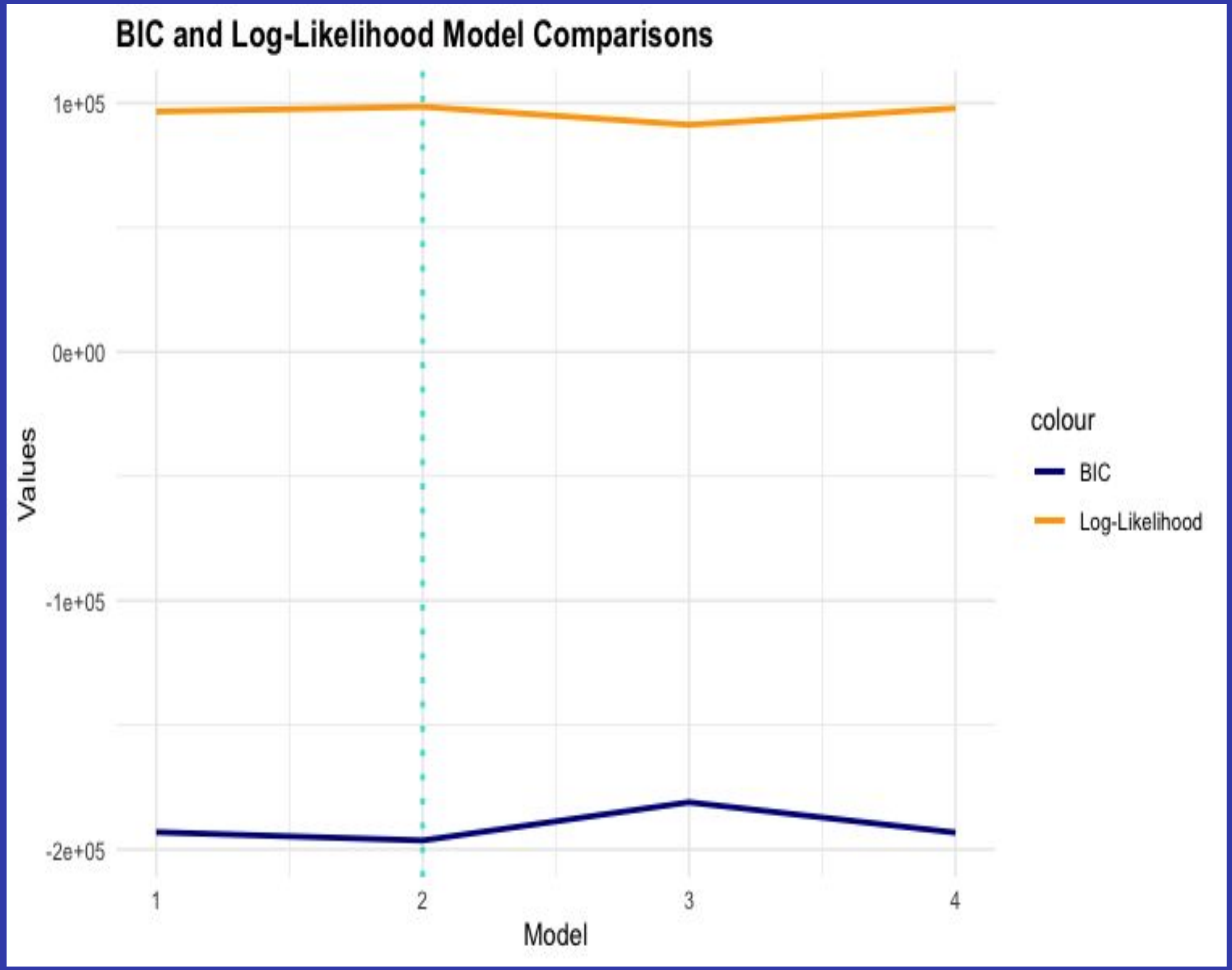
We chose a 70/30 proportion split for train and test respectively.

Log-Likelihood

Log-likelihood in HMMs gives us a measure of the performance of the model fit and helps in understanding the state observations.

Bayesian Information Criterion (BIC)

BIC offers a good measure to decide the best model given its increasing complexity, avoiding overfitting by estimating the model to the data provided.



FINDING THE MODEL

Before doing any Anomaly Detection, we had to find the most reliable and best results model

Best Model = High Log-LikeliHood and Low BIC

We calculated the difference as:

Difference = BIC - Log-Likelihood (all negative)

The best models had the smallest difference.

In the end, the best model had **n_states = 24**

Initial Models

We started with 6 models from 4 to 24, in increments of 4 each time

More Models

After inspecting the Log-Like of all 6 models, we saw that n_states = 16, 20 and 24 were the best. We decided to make 5 more models in-between those values

Test Data Comparison

Using the 3 best models, we did forwardbackward substitution with the test data to get the log-like. Then normalized the log-likes by dividing by dataset size. The best model for both LL was chosen for anomaly detection

Using HMMs for Anomaly Detection

Lower log-likelihood = values don't match with the expected behaviour of data set

lower log-likelihood = more anomalous data

We found that the **3rd data set** had the lowest LL and therefore contains the most anomalies.

1. Filter Datasets

We completed the same feature engineering (except. PCA analysis) on the 3 datasets

2. Create Model

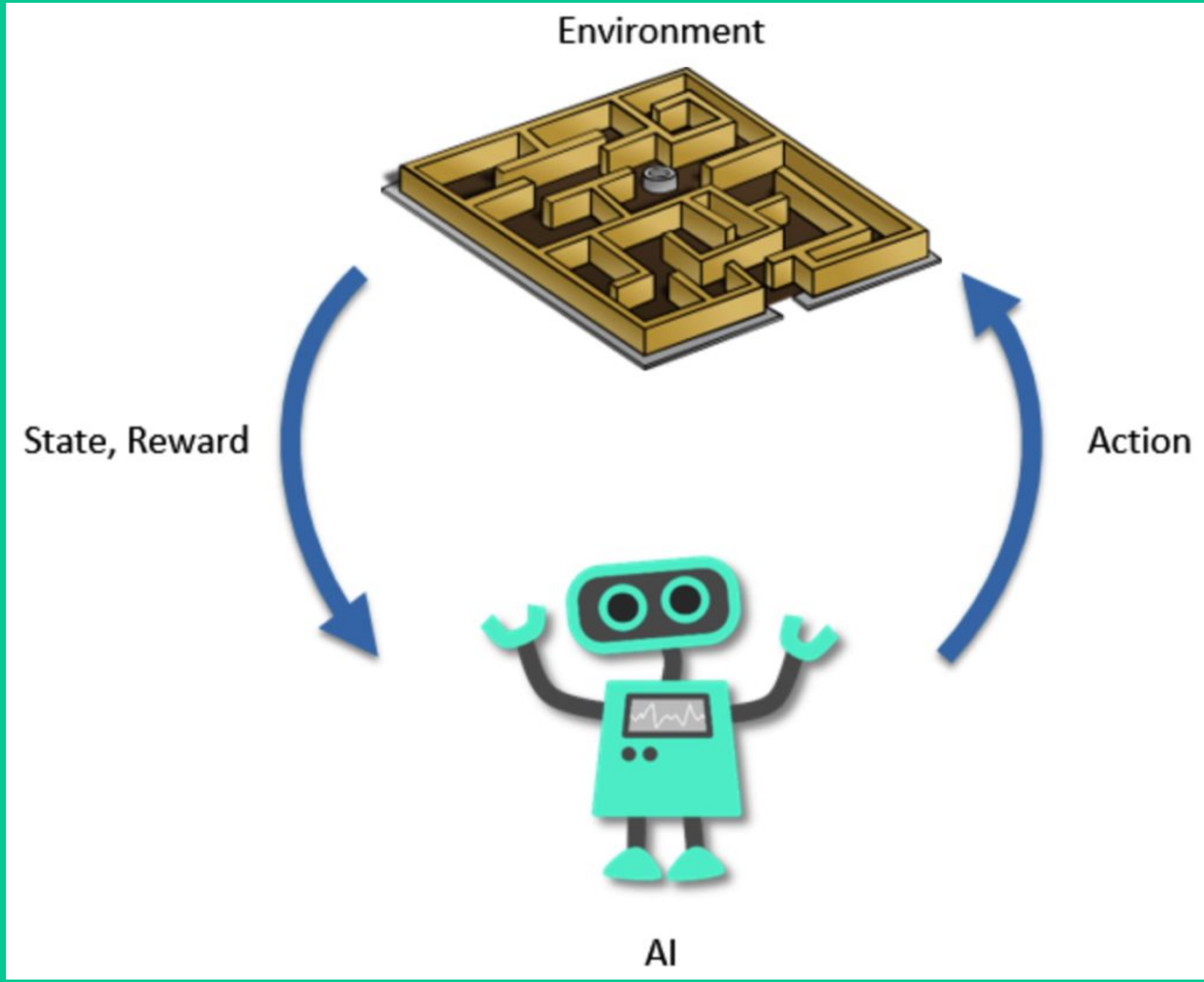
Using the best n_states value we got during the last set (n_states = 24), We created 3 HMMs for each anomalous dataset.

3. Compute Log-Likelihood

Using the built-in method, we computed the log-like for each model

Reinforcement Learning

- Reinforcement Learning is a Machine Learning algorithm based on state, action and reward.
- In this environment, given a state the goal is to take actions in order to maximize cumulative reward in the end.
- In the cybersecurity realm, RL systems can be trained for intrusion detection by identifying abnormal behaviour and responding to malware accordingly.



https://hub.packtpub.com/wp-content/uploads/2019/12/reinforcement-learning-1024x835.png

Hyperparameter Choices

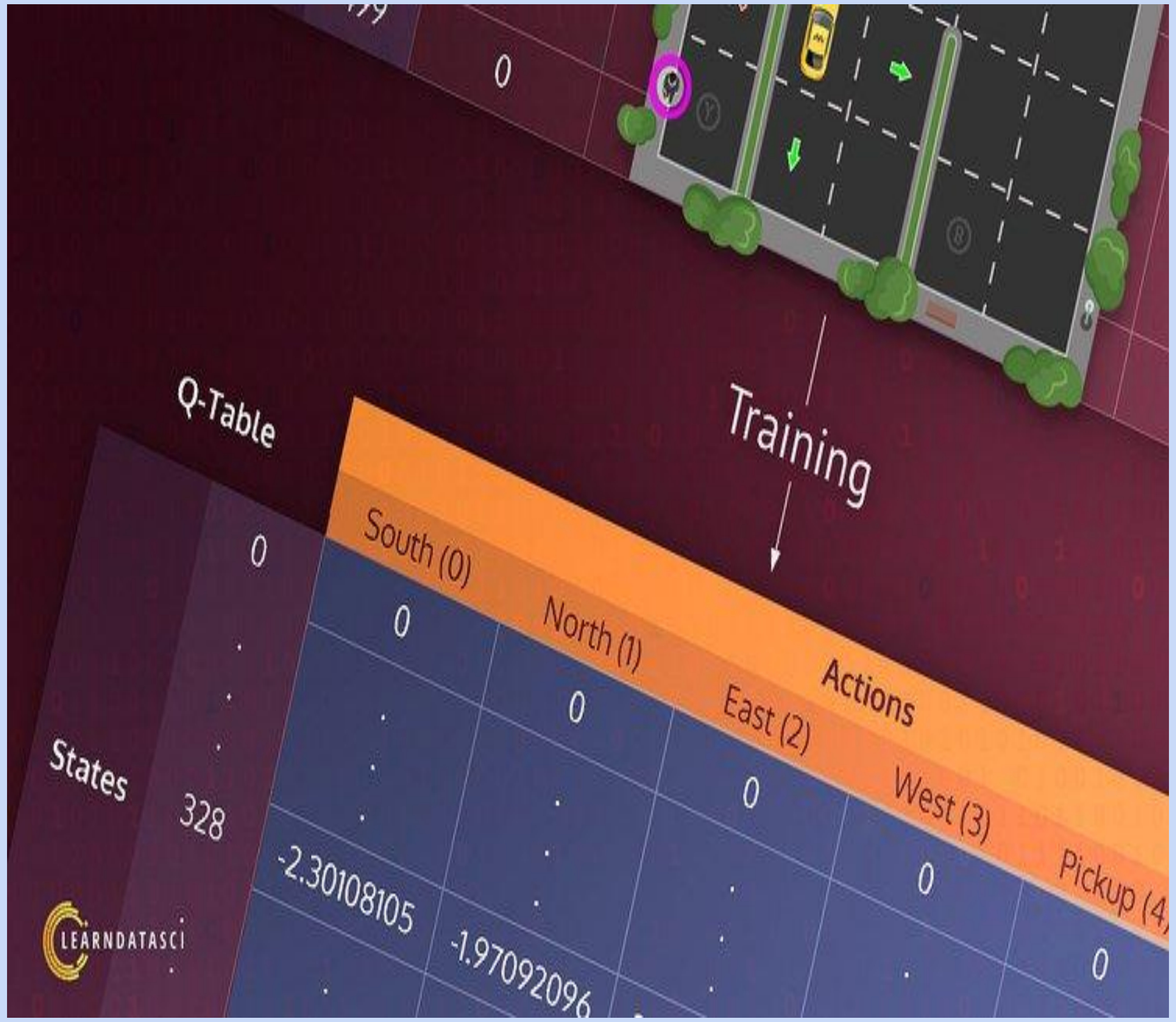
- **Alpha (α)** represents the model's learning rate
  - We chose alpha value = 0,2

- **Gamma (γ)** is the 'discount factor,' determining the weight assigned to future rewards as compared to immediate rewards.
  - We chose gamma value = 0.6

- **Epsilon (ϵ)** defines the exploration process in the greedy-action selection procedure.
  - We chose epsilon value = 0.2

Q-table Analysis

- Reward is almost always positive.
- Commodities and Real-Estate exhibit the widest ranges
  - They also average the highest q-values
- Forex and Stock values have moderate to high q-values
  - Are generally in the mid-range with moderate variability
- Cryptocurrencies and Stocks tend to average the lowest q-values
  - Cryptocurrencies vary from having both positive and negative q-values.



https://www.learndatasci.com/tutorials/reinforcement-q-learning-scratch-python-openai-gym/

Policy Results Analysis

```
> computePolicy(model)
             48                49                50                51                52                53                54                55 
  "Commodities"           "Forex" "Cryptocurrencies"          "Stocks"    "Real_Estates"           "Forex"   "Commodities"           "Forex" 
             56                57                58                59                60                61                62                63 
        "Forex" "Cryptocurrencies" "Cryptocurrencies" "Cryptocurrencies"   "Commodities" "Cryptocurrencies"   "Commodities"    "Real_Estates" 
             64                65                66                67                68                69               100                70 
 "Real_Estates" "Cryptocurrencies"          "Stocks"          "Stocks"           "Forex"     "Commodities"   "Commodities"    "Real_Estates" 
             71                72                73                74                75                76                77                78 
  "Commodities"    "Real_Estates" "Cryptocurrencies"     "Commodities"          "Stocks"    "Real_Estates" "Cryptocurrencies"          "Stocks" 
              1                79                 2                 3                 4                 5                 6                 7 
  "Commodities"           "Forex"    "Real_Estates" "Cryptocurrencies"    "Real_Estates"    "Real_Estates"           "Forex"    "Real_Estates" 
             10                 8                80                11                 9                81                12                82 
  "Commodities"    "Real_Estates"          "Stocks"     "Commodities" "Cryptocurrencies"    "Real_Estates"    "Real_Estates"    "Real_Estates" 
             13                83                14                84                15                85                16                86 
 "Real_Estates"     "Commodities"    "Real_Estates"          "Stocks"    "Real_Estates"          "Stocks"    "Real_Estates"           "Forex" 
             17                87                18                88                19                89                20                90 
 "Real_Estates"     "Commodities"     "Commodities"          "Stocks"          "Stocks" "Cryptocurrencies"    "Real_Estates"          "Stocks" 
             21                91                22                92                23                93                24                94 
  "Commodities"          "Stocks"    "Real_Estates"           "Forex" "Cryptocurrencies" "Cryptocurrencies"   "Commodities" "Cryptocurrencies" 
             25                95                26                96                27                97                28                98 
 "Real_Estates"     "Commodities"    "Real_Estates"           "Forex"     "Commodities"           "Forex"   "Commodities"          "Stocks" 
             29                99                30                31                32                33                34                35 
 "Real_Estates"           "Forex"     "Commodities"    "Real_Estates"           "Forex"          "Stocks"         "Forex"     "Commodities" 
             36                37                38                39                40                41                42                43 
  "Commodities"          "Stocks"           "Forex"    "Real_Estates"    "Real_Estates" "Cryptocurrencies"    "Real_Estates"     "Commodities" 
             44                45                46                47 
 "Real_Estates" "Cryptocurrencies"     "Commodities"          "Stocks" 
```

Policy Results Analysis

- Displays the **optimal action** to take at each state, maximizing expected cumulative reward.
- Each state has been assigned its optimal action/investment sector
- Useful when determining which sector to invest in given a specific budget
- Policy also produces a high, positive reward of 12033.83 suggesting that the investment/trading strategy is successful and produces a significant financial gain.

https://www.freepik.com/premium-vector/stock-market-concept-with-people-scene-flat-cartoon-design-man-makes-money-exchange-with-successful-strategy-analyzes-data-increases-profit-vector-illustration-visual-story-web_30250511.htm

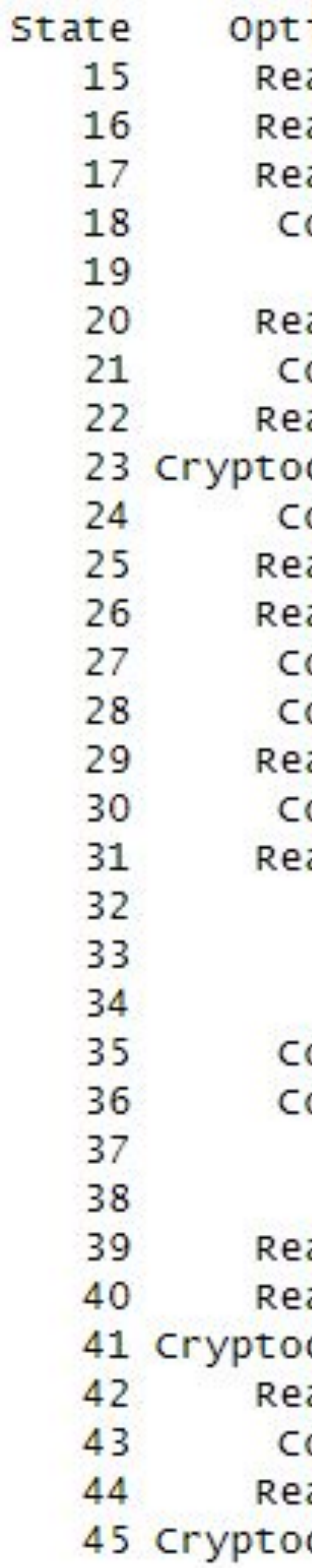
Behaviour towards Unseen Data

TASK:

- We trained the reinforcement model on the unseen data given the specified budget range ($15 - $45 million)

KEY HIGHLIGHTS:

- Real-estate is a very lucrative investment sector, being the optimal action for the most number of states.
- Cryptocurrency and Forex are less lucrative and only appear to do well in a select few states....invest with caution
- Commodities also appears to do well in a select states and are distributed across the state range



State	Opt
15	Rea
16	Rea
17	Rea
18	Co
19	
20	Rea
21	Co
22	Rea
23	Crypto
24	Co
25	Rea
26	Rea
27	Co
28	Co
29	Rea
30	Co
31	Rea
32	
33	
34	
35	Co
36	Co
37	
38	
39	Rea
40	Rea
41	Crypto
42	Rea
43	Co
44	Rea
45	Crypto

CONCLUSION

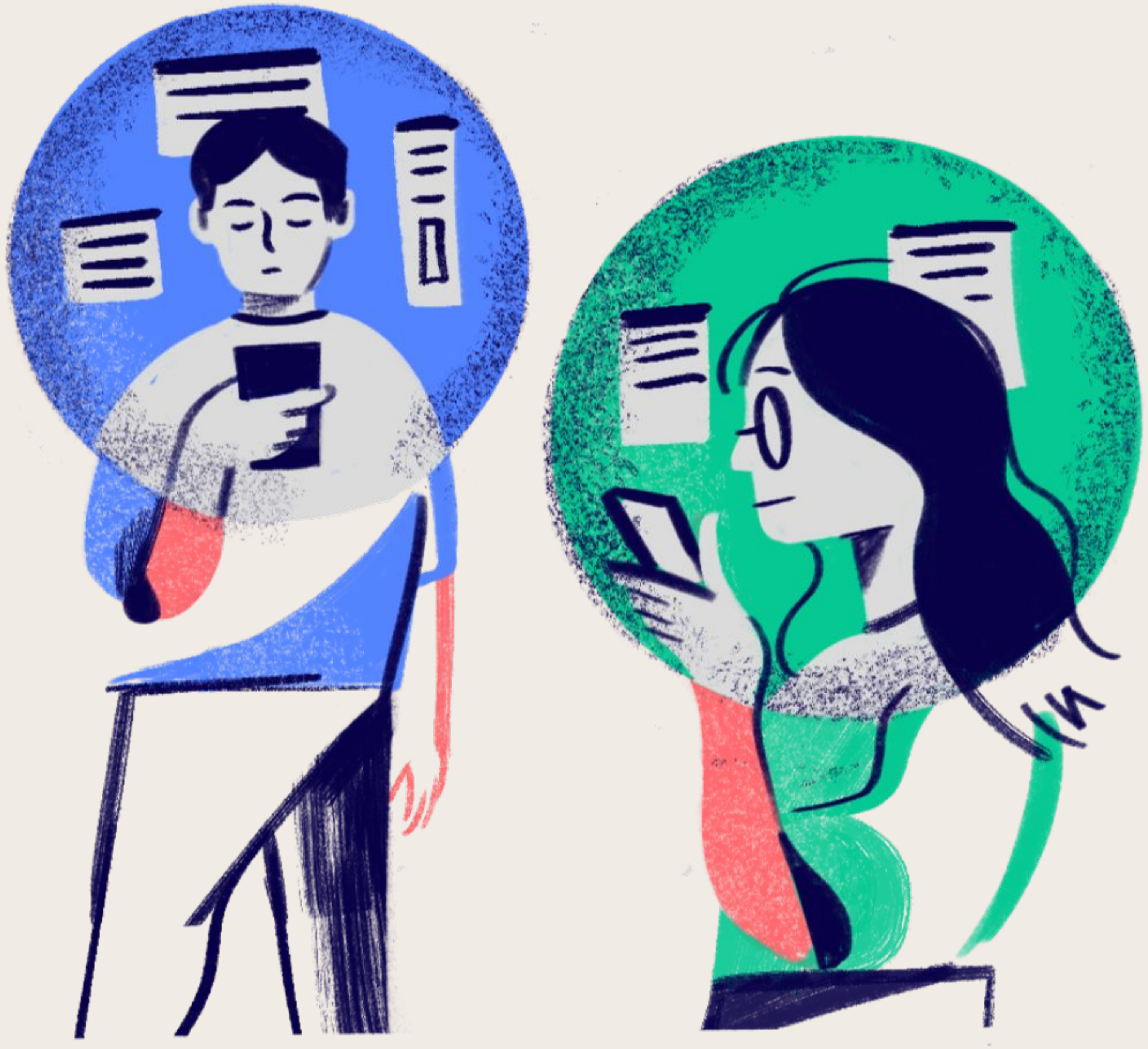
https://safetyandsecurityafrica.com/what-are-intrusion-detection-systems/

- Using feature engineering and probabilistic models like **HMMs** can help understand the data better to detect unusual behaviours indicative of security threats and malware.

- Machine learning models like **Reinforcement Learning** can help increase the efficiency of IDS in detecting malware by learning through the shortcomings, maximizing reward for safe and secure software solutions.

PRESENTED BY GROUP 24

THANK YOU VERY MUCH!



CMPT 318 - Fall 2023