Machine Learning for Cyber Security

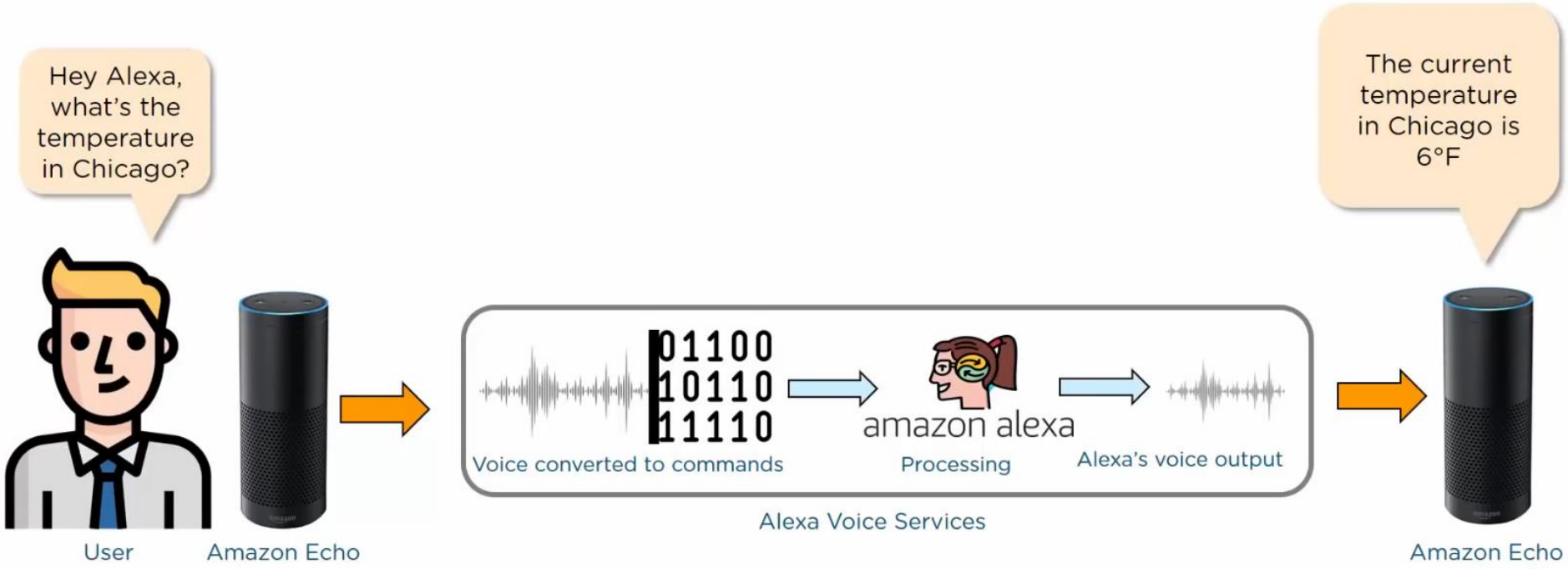
Objectives

- Why Machine Learning
- Artificial Intelligence vs Machine Learning vs Deep Learning
- What Is Machine Learning
- Why Machine Learning for Cyber Security
- How Machine Learning Works
- What Are Performance Metrics
- What Machine Learning Can Do
- Types of Machine Learning
  - Supervised Learning
  - Unsupervised Learning
  - Reinforcement Learning
- Linear Regression
- Decision Trees
- Support Vector Machine

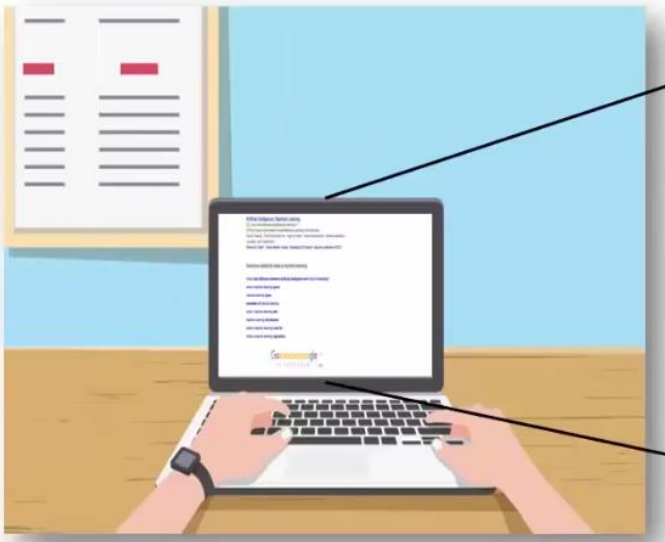
Why Machine Learning

Machine learning (ML) is a field of study in artificial intelligence concerned with the development and study of statistical algorithms that can learn from data and generalise to unseen data and thus perform tasks without explicit instructions

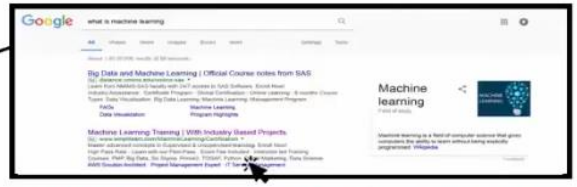
Artificial Intelligence vs Machine Learning vs Deep Learning



Artificial Intelligence vs Machine Learning vs Deep Learning



User searches for something on Google



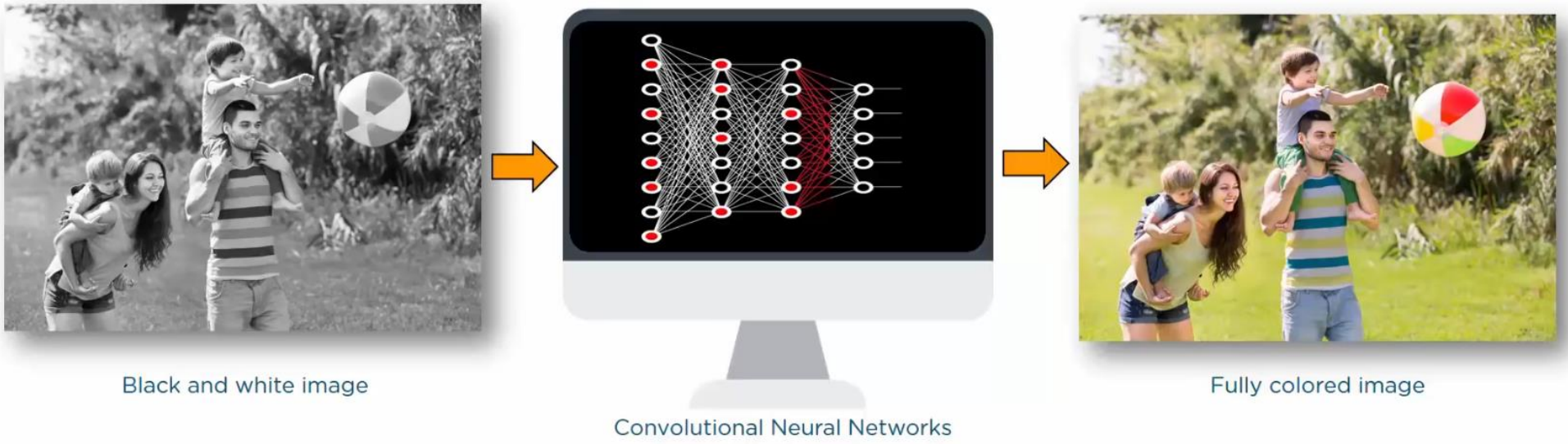
User selects one of the first few links and spends time there

User goes to the second/ third page

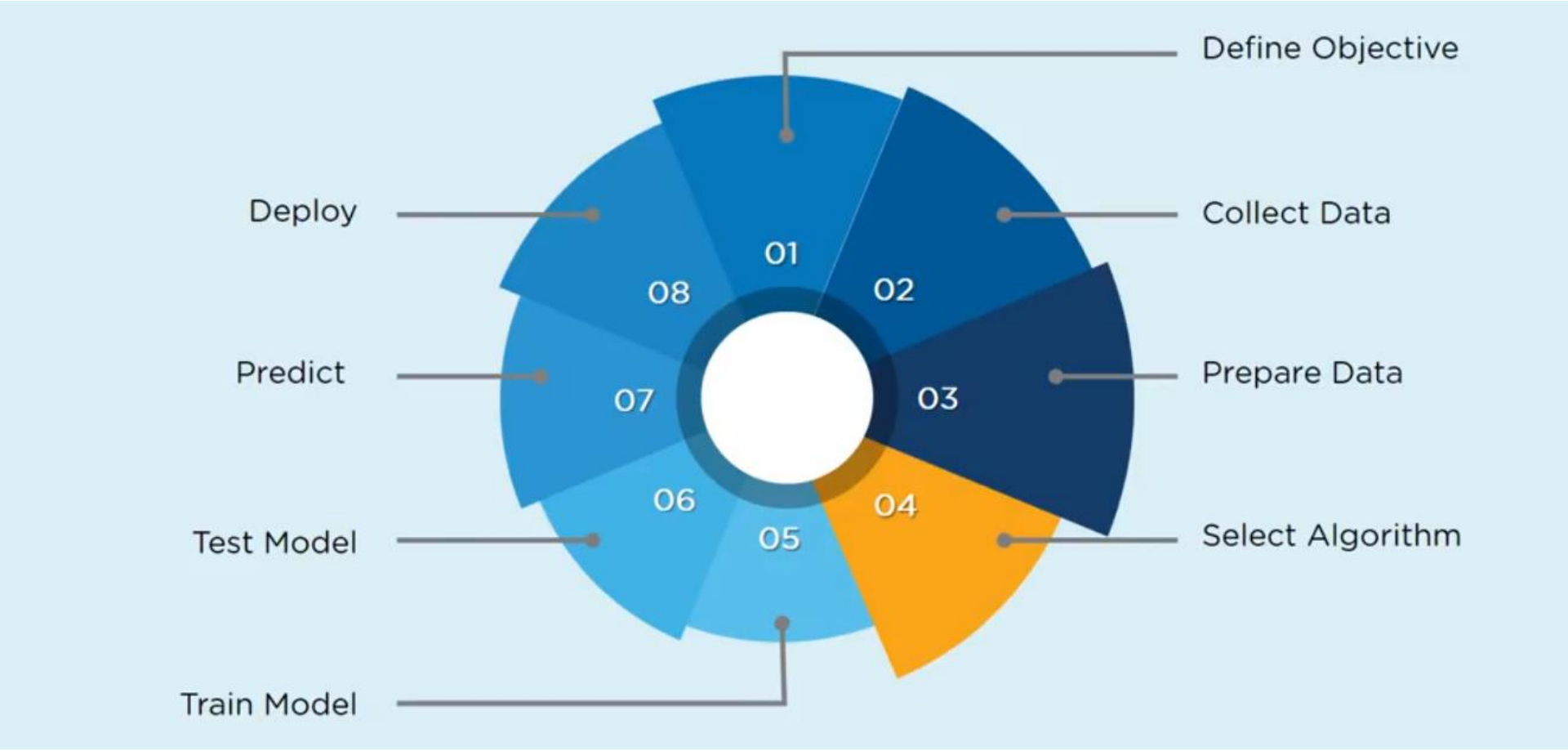
Google understands the user got what was required

Google understands the user's requirement wasn't satisfied

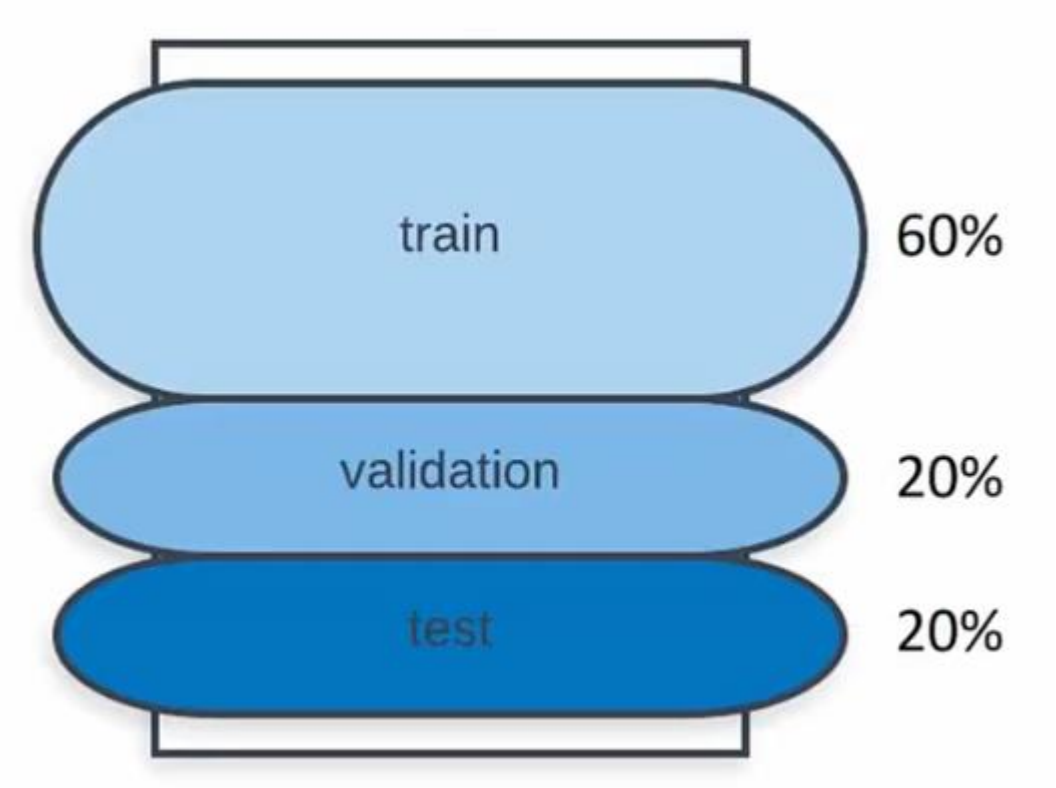
Artificial Intelligence vs Machine Learning vs Deep Learning



How Machine Learning Works

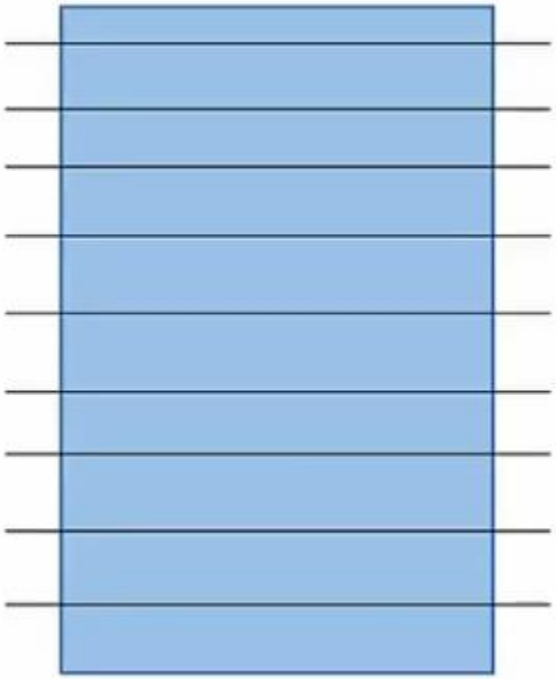


What Are Performance Metrics

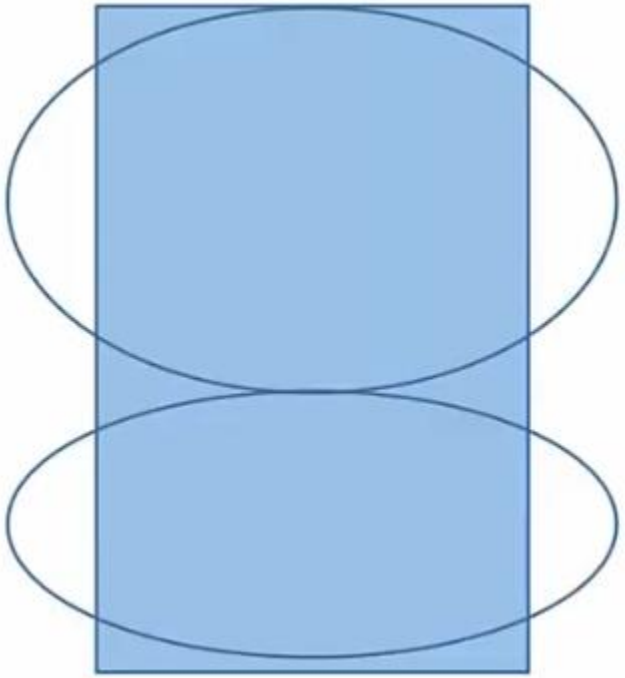


What Are Performance Metrics

10-fold cross validation



80%, 20%



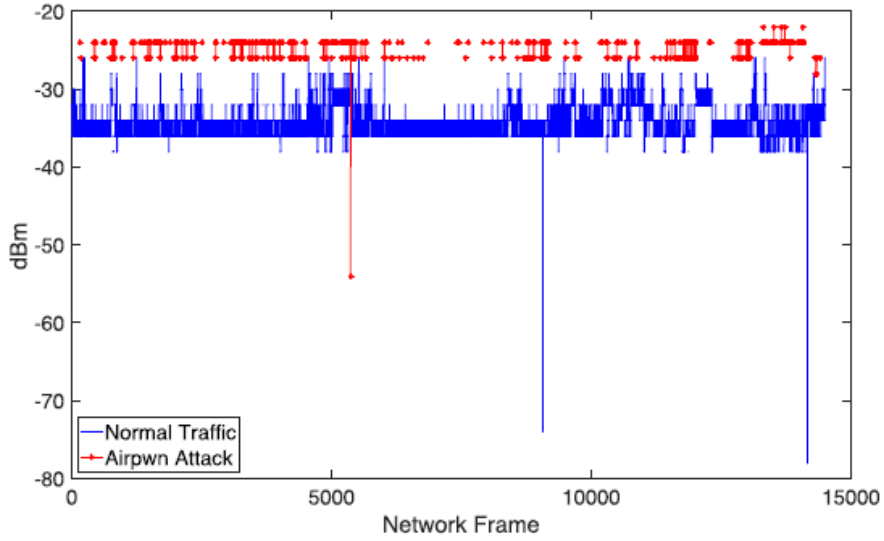


FIGURE 6. RSSI - Received signal strength measured by the victim machine during implementation of the MitM attack.

VI. EVALUATION OF RESULTS

This section describes the off-line detection results, and compares the results generated by the proposed methodology using all the possible combinations of metrics. There are two main purposes of these results. First, to evaluate the efficiency of the proposed methodology in identifying the presence of attacks, and producing reduced number of false alarms. Second, to identify which of the possible combinations of metrics produces the best detection results.

The effectiveness of the proposed methodology has been evaluated using the following performance metrics, which provide evidence of how effective an IDS is at making correct detections:

Network Frame

FIGURE 8. IAT - Inter arrival time difference between two consecutive frames, measured by the victim machine during implementation of the MitM attack.

- True Positive Rate (TPR) or Detection Rate - Proportion of malicious frames correctly classified among all the malicious data:

$$TPR = \frac{TP}{TP + FN} \tag{18}$$

- False Positive Rate (FPR) - Proportion of normal data misclassified as malicious among all the normal data:

$$FPR = \frac{FP}{TN + FP} \tag{19}$$

- Overall Success Rate (OSR) or Accuracy - Proportion of frames correctly classified among all the data:

$$OSR = \frac{TP + TN}{TP + FP + TN + FN} \tag{20}$$

- *Precision* - Proportion of malicious frames correctly classified among all the alarms generated:

$$Precision = \frac{TP}{TP + FP} \tag{21}$$

- *F*-score - Tradeoff between *Precision* and TPR, used to compare two distinctive classification methodologies:

$$F\text{-}score = \frac{2 \cdot Precision \cdot TPR}{Precision + TPR} \tag{22}$$

What Are Performance Metrics

where True Positive (TP) represents attacks classified as attacks; True Negative (TN) represents normal instances classified as normal; False Positive (FP) represents normal instances misclassified as attack; and False Negative (FN) represents attacks misclassified as normal.

We have divided the datasets in 80% for training (i.e. *train* data) and 20% for testing (i.e. *test* data). The training dataset was used to build the normality and attack baselines (i.e. *baseline* data), whereas the remaining data were used to generate the beliefs and evaluate the proposed methodology.

Since the attacker would use a low transmission rate, the NAV value set by the attacker would equivalently be larger than the NAV value set by the legitimate wireless devices.

From the presented results, it would be expected to use the single metric methodology using either *Rate* or *NAV* to defend the wireless network against MitM attacks at the physical layer. Nonetheless, the detection system cannot assume the implementation parameters chosen by the attacker. More importantly, it is impossible to anticipate the particular type of attack implemented by the attacker. Hence, basing the wireless injection attack detection on the use of single metric may be prone to a high number of misclassification results.

I. Ghafir et al., "A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection," IEEE Access, vol. 6, pp. 40008-40023, 2018. https://ieeexplore.ieee.org/document/8409949

What Machine Learning Can Do

Do you want to predict a category? That's classification!

For instance, whether the stock price will increase or decrease

What Machine Learning Can Do

Do you want to predict a quantity? That's regression!

For instance, predicting the age of a person based on the height, weight, health and other factors

What Machine Learning Can Do

Do you want to detect an anomaly? That's anomaly detection!

For instance, you want to detect money withdrawal anomalies

What Machine Learning Can Do

Do you want to discover structure in unexplored data? That's clustering

For instance: Finding groups of customers with similar behavior given a large database of customer data containing their demographics and past buying records

Categories of Machine Learning

- Supervised learning

Relies on labelled data to train models for classification or regression tasks, such as predicting house prices or identifying spam emails

- Unsupervised learning

Works with unlabelled data to discover hidden patterns
often using clustering, association, or dimensionality reduction techniques.

- Semi-supervised learning

Combines elements of both, using a small portion of labelled data to guide the learning process.

- Reinforcement learning

Mimics human learning by rewarding correct decisions and penalizing mistakes, allowing an agent to refine its actions over time to achieve the best outcome.

Types of Machine Learning

Types of Supervised Learning

Classification

When the output variable is categorical i.e. with 2 or more classes (yes/no, true/false), we make use of classification

Regression

Relationship between two or more variables where a change in one variable is associated with a change in other variable

Types of Machine Learning

Types of Unsupervised Learning

Clustering

The method of dividing the objects into clusters which are similar between them and are dissimilar to the objects belonging to another cluster

Association

Discovering the probability of the co-occurrence of items in a collection

Types of Machine Learning

Supervised vs Unsupervised Learning

Supervised learning:

- Labeled data
- Direct feedback
- Predict output

Unsupervised learning:

- Non-labeled data
- No feedback
- Find hidden structure in data

Acknowledgement

This material uses resources from:

- Virmani, C., Choudhary, T., Pillai, A. and Rani, M., 2020. Applications of Machine Learning in Cyber Security. In Handbook of Research on Machine and Deep Learning Applications for Cyber Security (pp. 83-103). IGI Global.
- Iyer, S.S. and Rajagopal, S., 2020. Applications of Machine Learning in Cyber Security Domain. In Handbook of Research on Machine and Deep Learning Applications for Cyber Security (pp. 64-82). IGI Global.
- THOMAS, T.P.V., Vijayaraghavan, A.P. and Emmanuel, S., 2020. MACHINE LEARNING APPROACHES IN CYBER SECURITY ANALYTICS. SPRINGER VERLAG, SINGAPOR.
- Verma, R.M. and Marchette, D.J., 2019. Cybersecurity Analytics. CRC Press.
- Machine Learning Tutorial. Simplilearn
- Gupta, B.B. and Sheng, Q.Z. eds., 2019. Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices. CRC Press.
- Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H. and Wang, C., 2018. Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, pp.35365-35381.
- Dua, S. and Du, X., 2016. Data mining and machine learning in cybersecurity. CRC press.