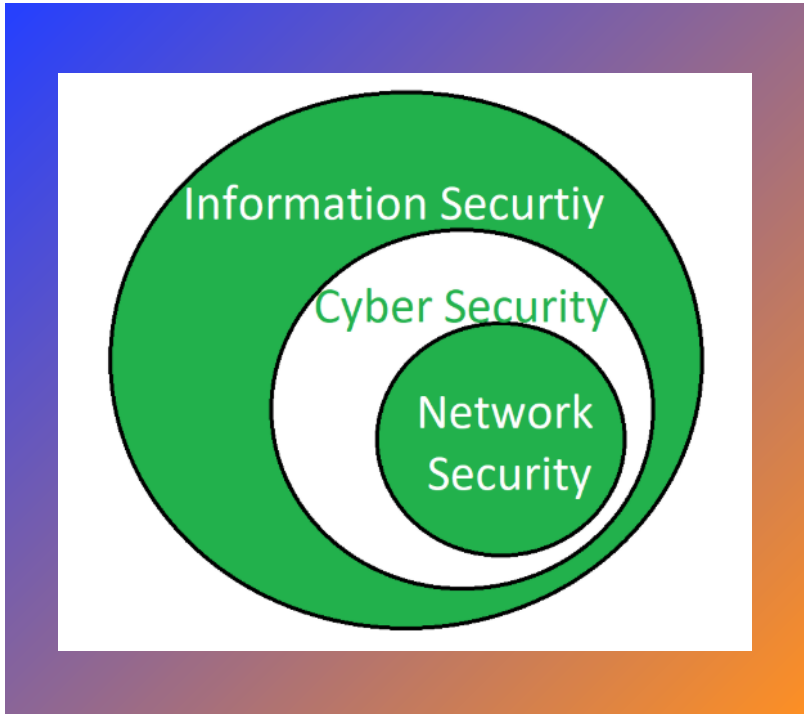
SECURING NETWORKS USING DEEP LEARNING BASED DETECTION SYSTEMS

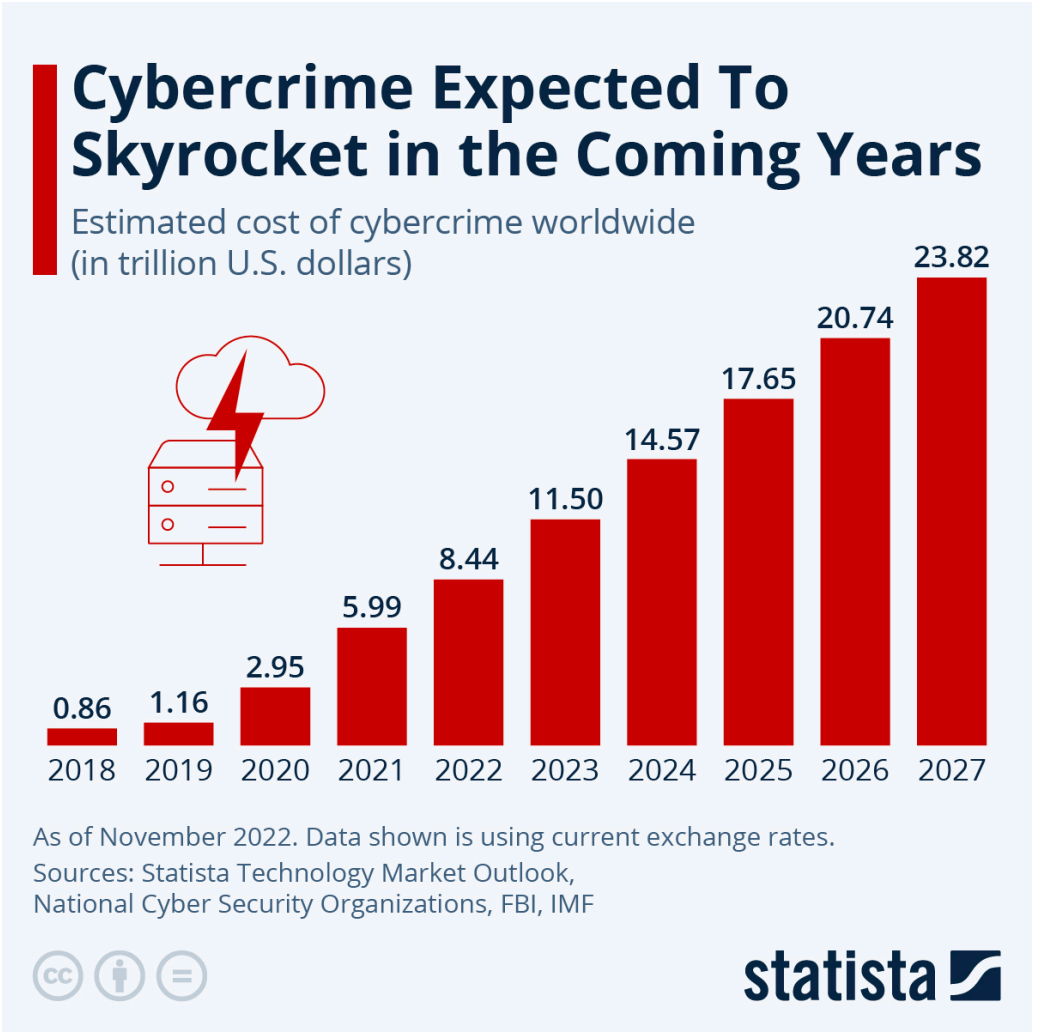
RITESH RATTI

Agenda

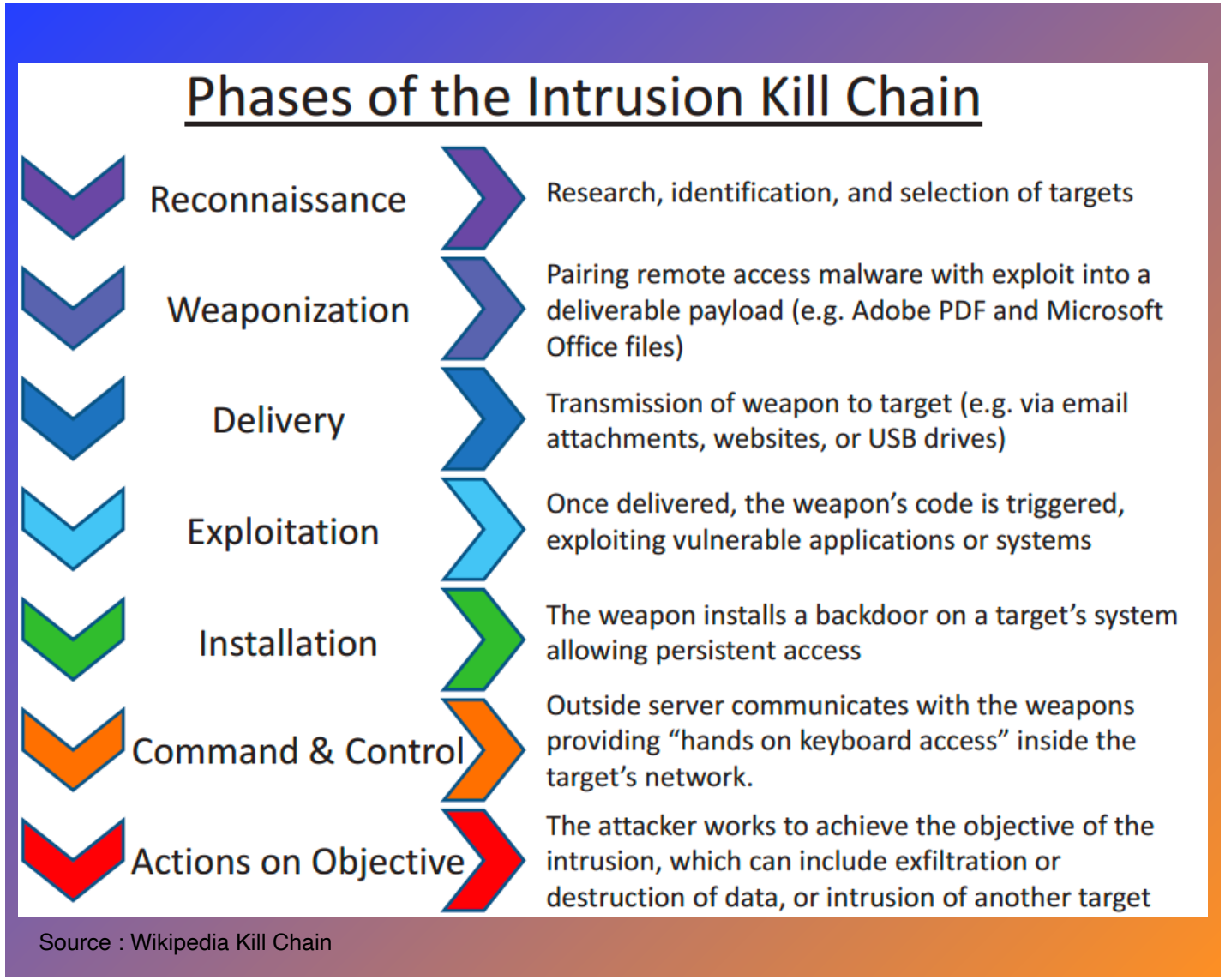
1. **Introduction to Network Security**
   Various attacks at TCP/IP layers / Attack Phases / Tools etc.
2. **What is Intrusion Detection System (IDS)**
   Definition / Types / ML Based IDS
3. **Deep Learning based IDS**
   Limitations / Introduction / Datasets
4. **Supervised DL based IDS**
   Multilayer Perceptron / RNN / CNN
5. **Unsupervised DL based IDS**
   Autoencoders / GANs

Introduction to Network Security



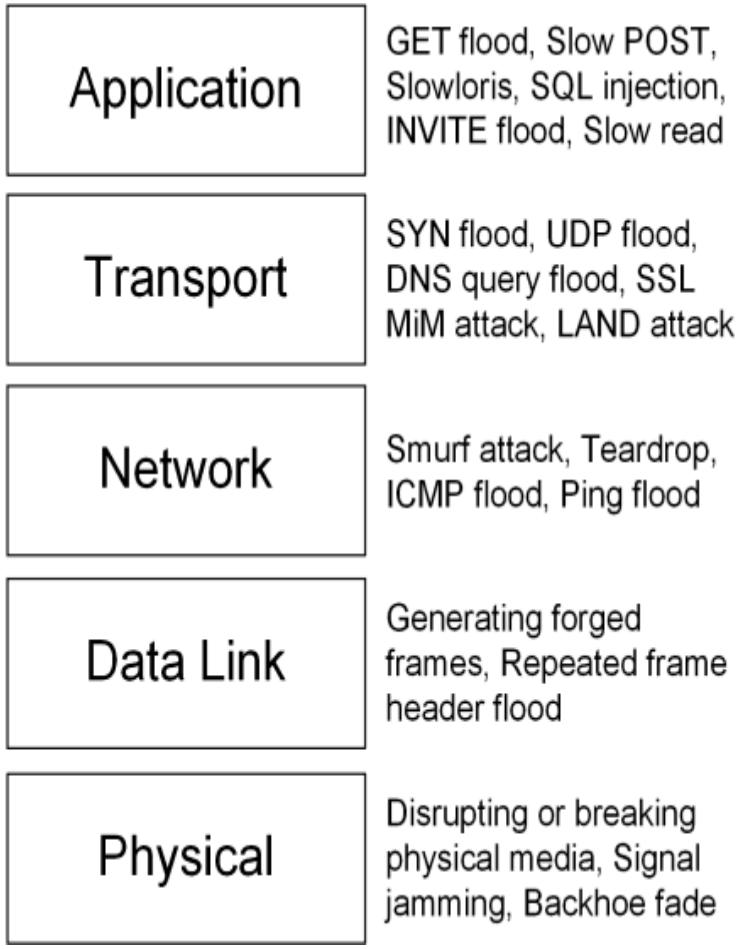


Various phases of Attacks



Source : Wikipedia Kill Chain

Various attacks at TCP/IP layers



- Tools
  - Ncrack
  - Cain and Abel
  - John the Ripper
  - Nmap
  - LOIC

What is Intrusion Detection System

- Intrusion detection is method to identify set of malicious actions that compromise the integrity, confidentiality and availability of information resources.
- Challenges
  - Detection Accuracy
  - Detection Speed
  - Dynamic Nature of Attacks
- Types
  - Supervised vs Unsupervised
  - Host Based vs Network Based
  - Packet Level vs Flow Level

Signature Based Methods

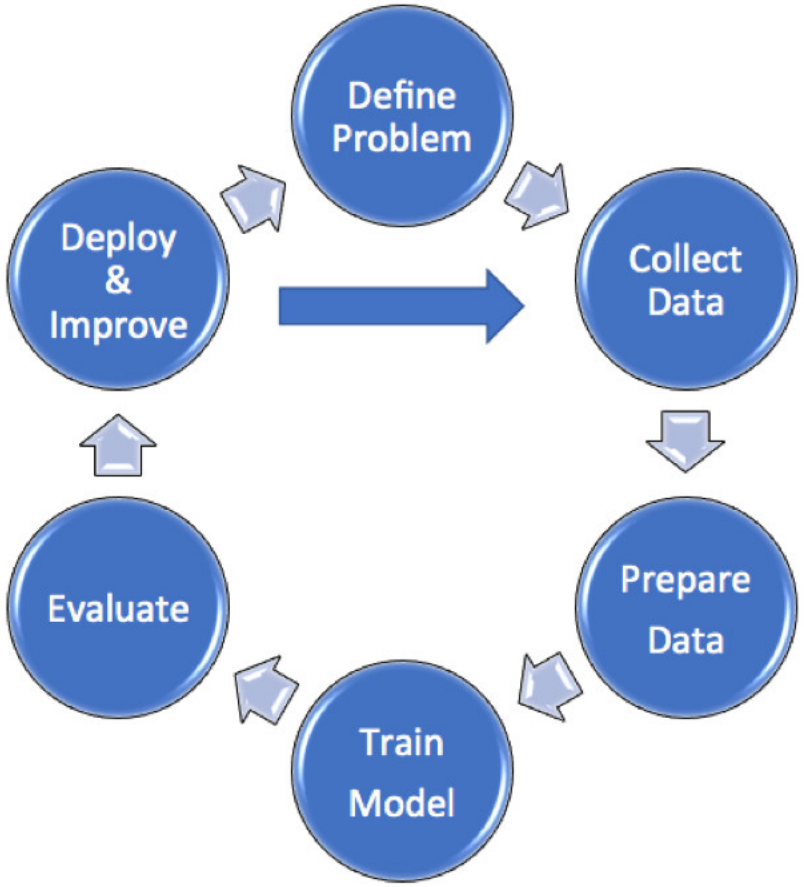
- Predefined rules and Signature to detect attack.
- Snort is a free and open-source network intrusion prevention and detection system. It uses a rule-based language used to detect malicious activity such as DoS, Buffer overflows, stealth port scans etc.

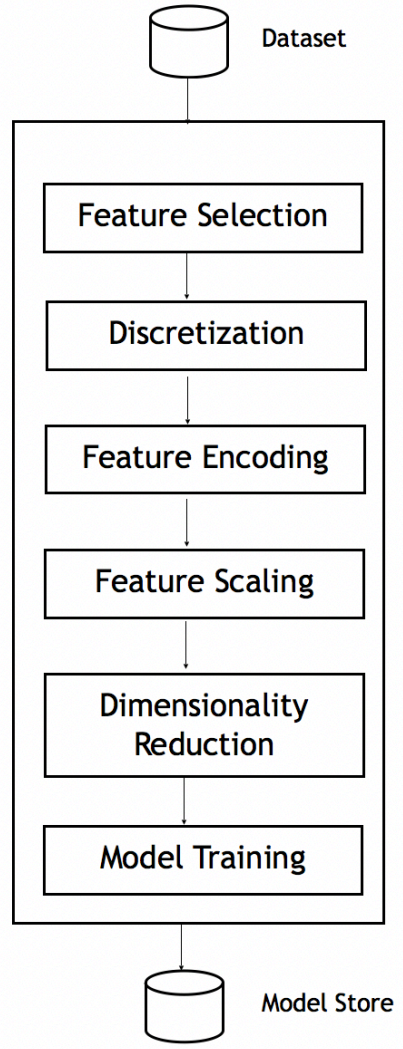
```
alert icmp any any -> $HOME_NET any (msg:"ICMP flood"; sid:1000001; rev:1;
classtype:icmp-event; detection_filter:track by_dst, count 500, seconds 3;)
```

- iptables : Command line utility to configure kernel packet filtering rules

iptables -A INPUT -p tcp -m connlimit --connlimit-above 80 -j REJECT --reject-with tcp-reset

Supervised Learning based methods

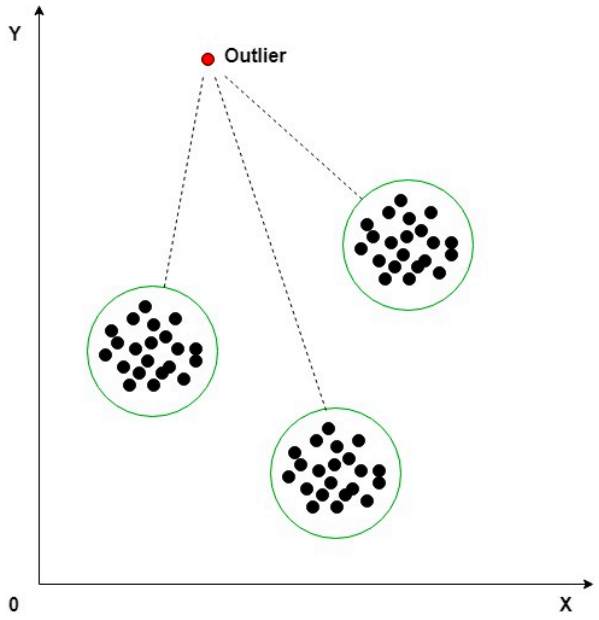


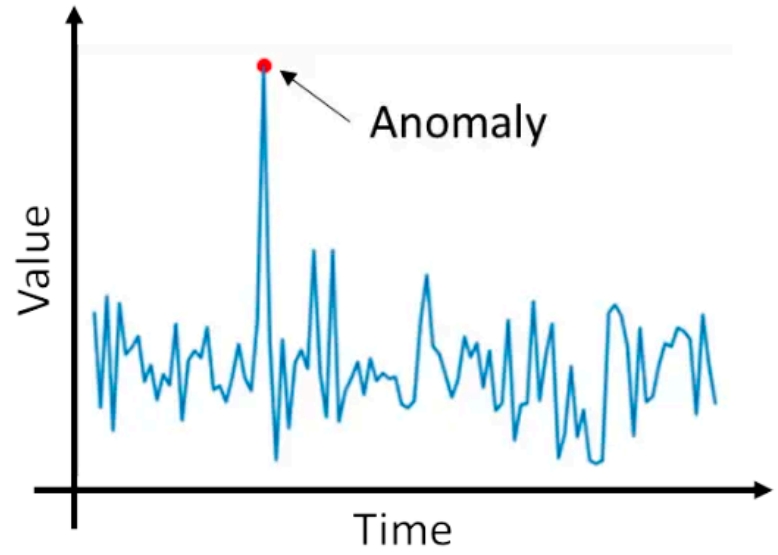


Unsupervised Learning based methods

Unsupervised learning-based IDS models benign behaviour of the system from the normal profile and any deviation from the known profile is considered an intrusion.

- Clustering Based
- Outlier Detection Based
- Statistical methods





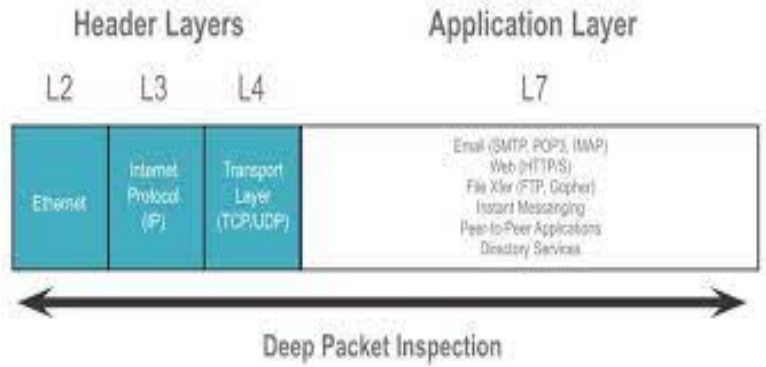
Comparison

Comparison of Supervised and Unsupervised learning based IDS

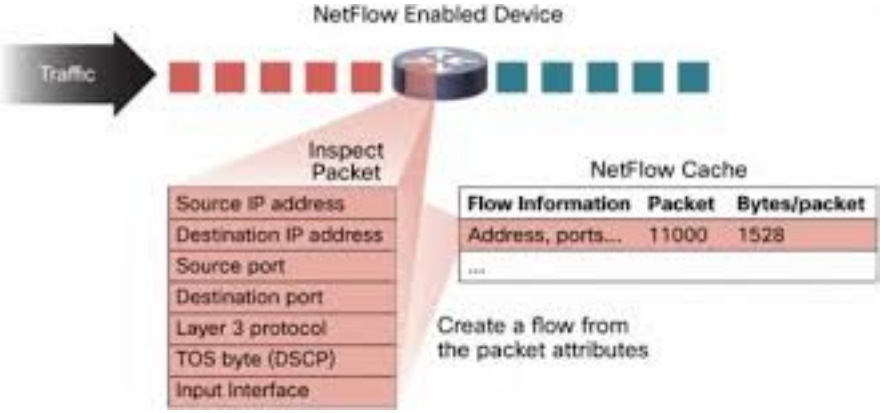
Method	**Data Requirement**	**Capture new attacks**	**Data Update**	**False Alarms**
Supervised Learning	Labelled Data is desired that involves huge manual labelling effort.	It is unable to capture the new attacks.	Frequent data update is needed.	Less number of false alarms are generated.
Unsupervised Learning	Labelled data is not required and model can be build on normal data alone.	It can capture new attacks and zero day attacks.	It does not require frequent data updates.	High number of false alarms are generated.

Packet Level IDS vs Flow Level IDS

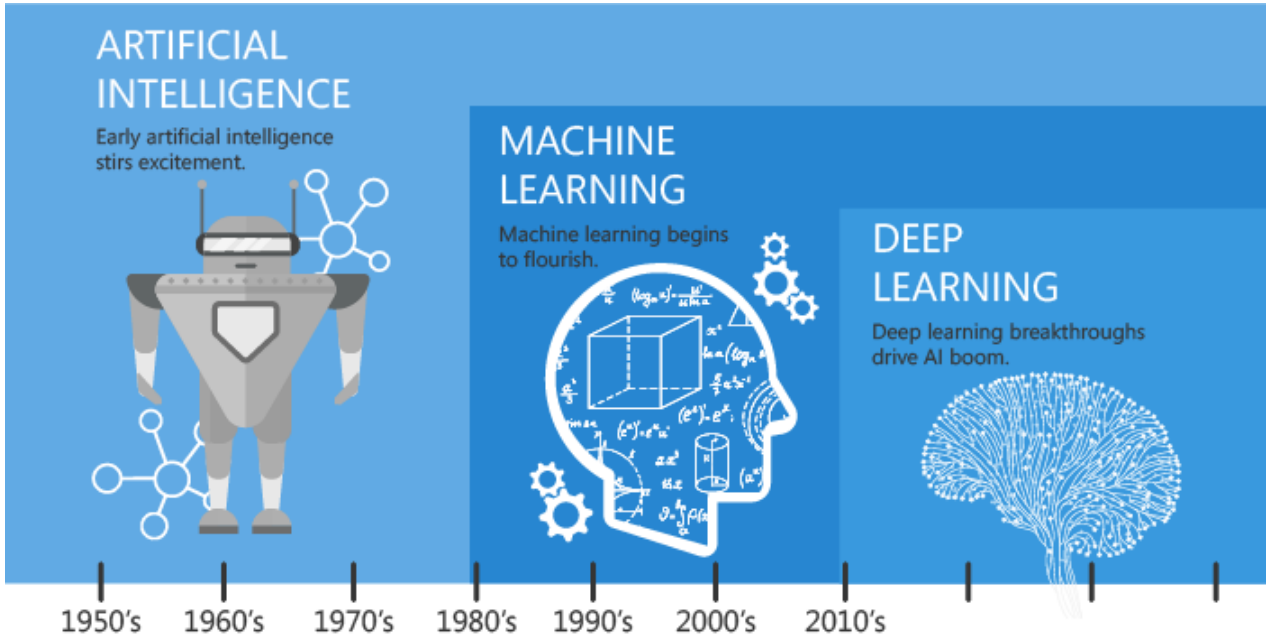
- Packet Level Detection
  - Capture the packet level information from network packets.
  - Generate label data based on attack timing.
  - Capture features based on packet level information like header information, application data etc.
  - Use Deep Packet inspection on encrypted networks.



- Flow level Detection
  - Capture Flow level information on discrete time windows using Netflow / CICFlowMeter etc.
  - Aggregate the information for each flow and create features like bytes per sec / packets per sec / Flow IAT / .
  - Use features to build machine learning model.

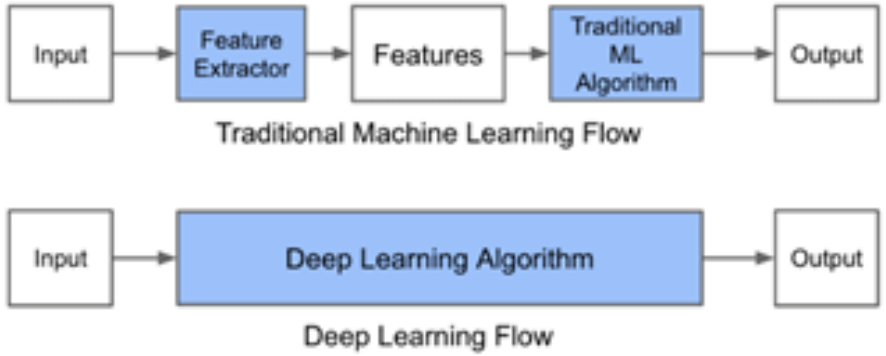


Deep Learning



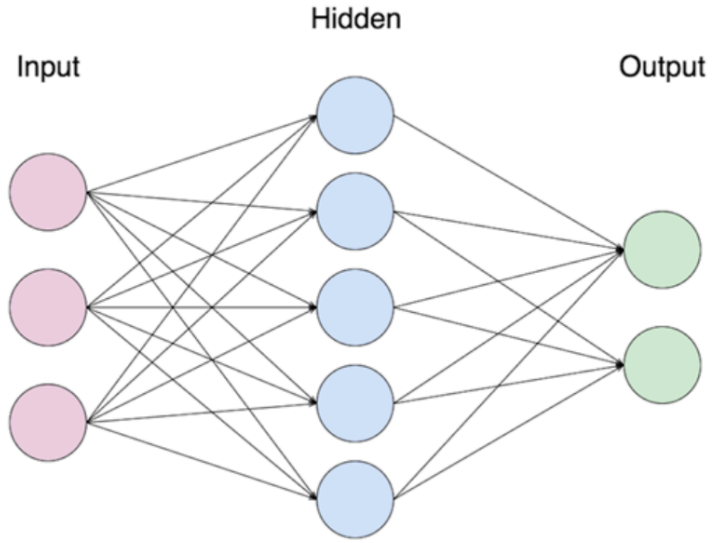
Traditional ML Limitations

- **Feature Selection**
  - Traditional approaches rely completely on feature selection hence immense time is invested in feature engineering.
- **Scalability**
  - Traditional approaches are non scalable with respect to big data.
  - Problem of overfitting for large data sets.
- **Hyper-parameter tuning**
  - Required extreme tuning for hyper parameters.
  - Decision of kernel for kernel based approaches.
  - Selection of optimisation parameters require.
- **Hierarchical Representation**
  - Missing hierarchical representation in most of the algorithms.



Deep Learning : Introduction

- Deep Learning is class of machine learning algorithms that
  - Use cascade of many layers for processing.
  - Each successive layer uses output from previous layer.
  - Higher level feature derived from lower level features.
- Deep Learning algorithms are based on distributed representations
  - Observed data are generated by the interactions of factors organized in layers.
- Deep Learning is a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain.
- Deep learning refers to artificial neural networks that are composed of many layers.

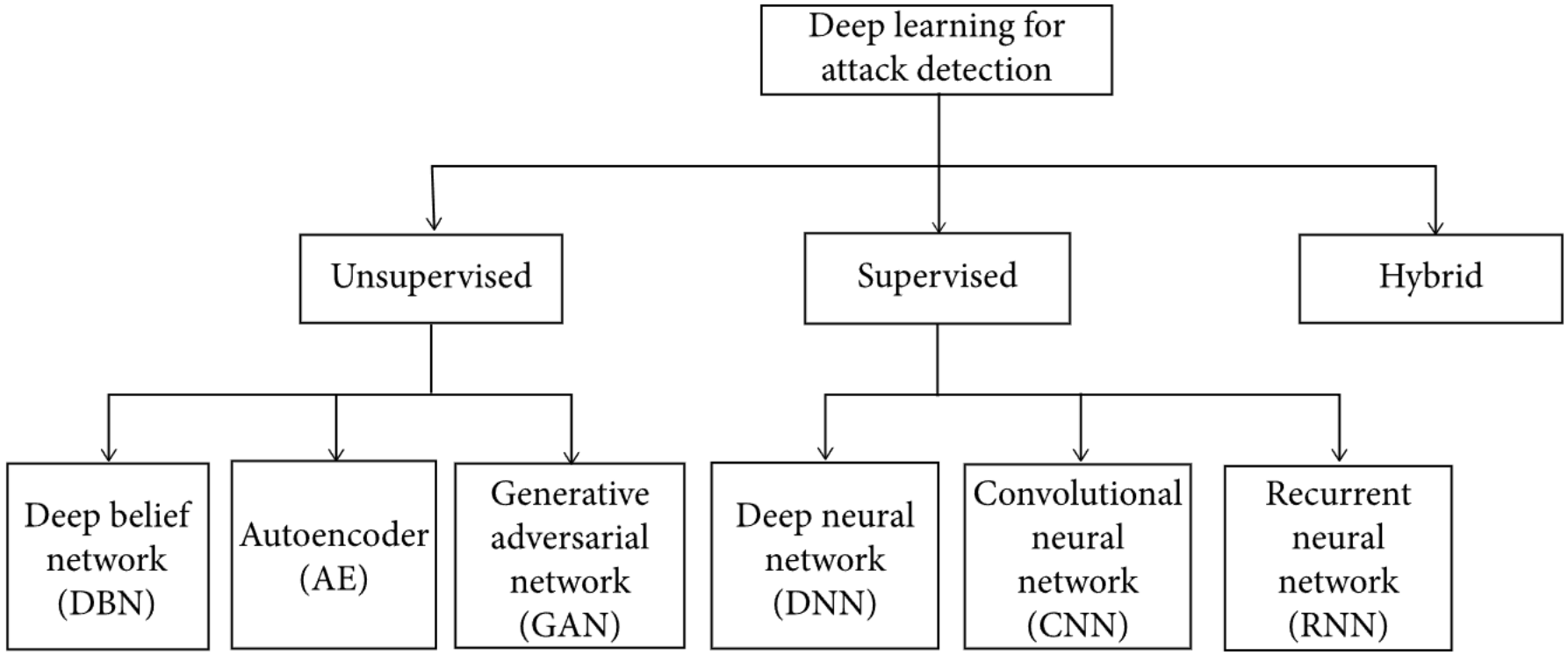


Datasets

Dataset	Year	Description
DARPA	1998	Developed by MIT Lincoln laboratory
KDD Cup	1999	Used for 3rd KDD Competition for attack classes like DoS, Probe, U2R, R2L
KYOTO dataset	2006	Traffic data from Kyoto university Honeypots
ITOC-CDX	2009	The Cyber Research Centre Datasets that provides a comprehensive set of log data under ongoing "sophisticated" attacks
NSL-KDD		This dataset is improved version of KDD dataset.
ADFA Dataset	2013	For host-based intrusion detection system (HIDS).
UNSW-NB15	2015	Developed by University of New South Wales, Australia using Bro IDS.
CICIDS-2018	2018	Recent data developed by Canadian Institute of Cyber Security
CIC-DDoS-2019	2019	DDoS attack for various Networking Protocols

Deep Learning based methods

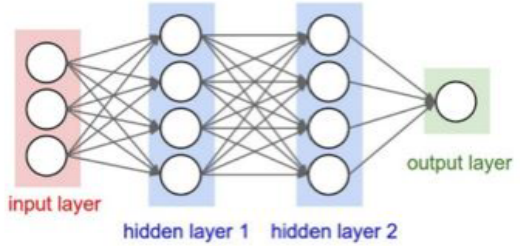
- Supervised
- Unsupervised
- Hybrid

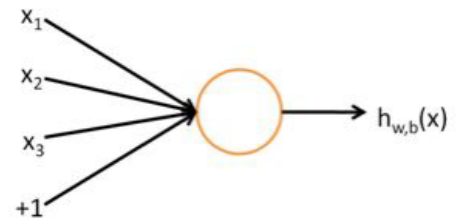


Supervised DL based methods

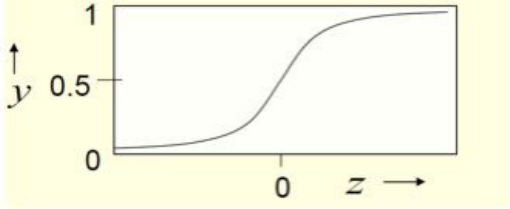
Deep Neural Network

- It is based on back propagation algorithm and contains input, output and various intermediate layers.
- Neurons are basic computation entities.
- Activation function is calculated at each layer in feed forward fashion and Error is propagated backwards for weight normalization.
- Adjust weight using gradient descent algorithm where it increment or decrement the weight vector by the input vector scaled by the residual error and the learning rate.
- Output layer is used to predict the outcome as attack or non-attack.





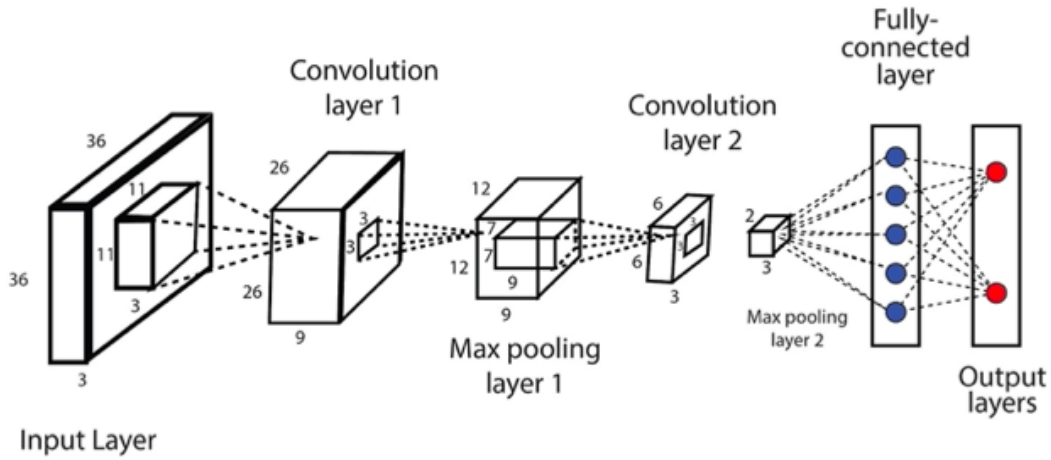
$$z = b + \sum_i x_i w_i \qquad y = \frac{1}{1+e^{-z}}$$



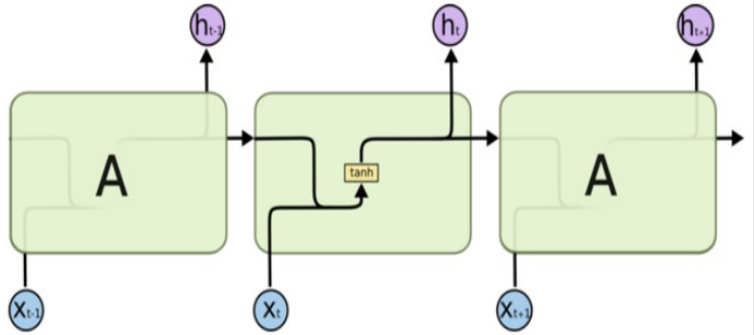
$$y = \varphi(\sum_{i=1}^{n} w_i x_i + b) = \varphi(\mathbf{w}^T \mathbf{x} + b)$$

Convolutional Neural Network

- Connection patterns are inspired by visual cortex in CNN.
- Convolutional layers are set of learnable filters where every filter is applied along width and height of 2-D vector. Pooling operation is used to reduce the learnable parameters.
- Various layers of convolutional networks are used and followed by fully connected layer to classify the input record into benign or attack.



Recurrent Neural Network

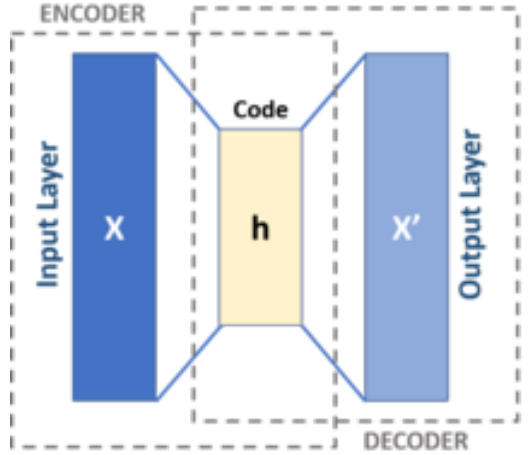


- This is Neural Network with directed cycles.
- It is based on recursive operation where Output of next layer become input to previous layer.
- RNNs capture patterns in time series data , Constrained by shared weights across neurons
- Recurrent Neural Network are natural way to model sequential data.
- Usage of intermediate memory gate.
  - Information gets into the cell whenever its write gate is on.
  - The information stays in the cell so long as its keep gate is on.
  - Information can be read from the cell by turning on its read gate.

Unsupervised DL based methods

Auto Encoder

- Autoencoder are unsupervised machine learning technique in which we leverage neural networks for representation learning.
- Encoder that maps the input into the code, and a decoder that maps the code to a reconstruction of the input.
- Use Cases :
  - Dimensionality Reduction
  - Representation Learning for classification tasks



Reconstruction Error Based

Autoencoder learn the representation for Normal Traffic . During execution time predict the Attack if reconstruction error is higher than threshold.

Triplet Loss Based

Learn representation from 2 encoders specifically for Attack and Normal data.
Use Triplet loss function for attack identification.

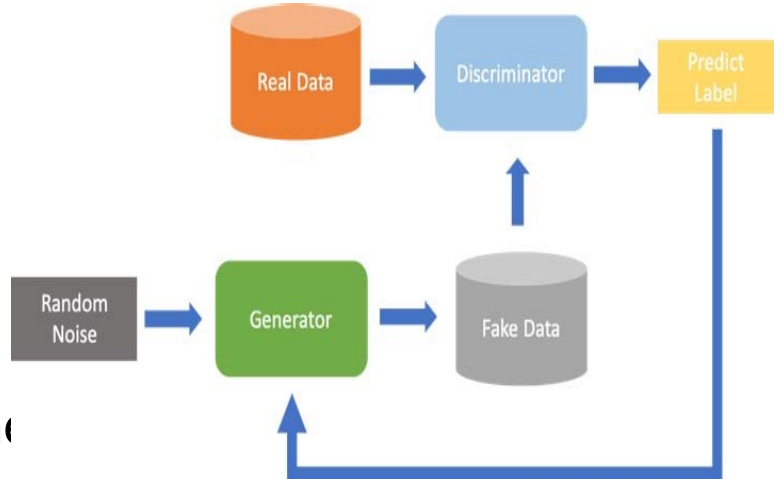
$$Loss = \sum_{i=1}^{N} \left[\|f_i^a - f_i^p\|_2^2 - \|f_i^a - f_i^n\|_2^2 + \alpha \right]_+$$

Generative Adversarial Networks

- Generative Adversarial Network (GAN) is a novel generative model, by learning the data distribution and represent it as latent variables

- The *Generative Network* generates candidates while the Discriminative Network evaluates them.

- The generative network's training objective is to increase th error rate of the discriminative network . This way the generator trains based on whether it succeeds in fooling the discriminator.



Oversampling Strategy

Malicious packets are extremely less than normal packets
GAN can be used for Oversampling in case of NIDS

Thanks