APPLICATION OF DEEP MACHINE LEARNING IN CYBERSECURITY

N. Kakumani, S. Tse,
S. Muniz
Advisor: Dr. Emamian

INTRODUCTION

Cybercrime is one of the world's fastest growing threats to security.

- Unfortunately corresponds to our growing dependence on computer networks and information technology (banking software, autonomous vehicles, smart assistants - Siri, Alexa)
- An estimated $6 trillion global cost by 2021 under the 2020 Official Annual Cybercrime Report by Cybersecurity Ventures

Silver Lining: New Deep Machine Learning Cybersecurity Tools…

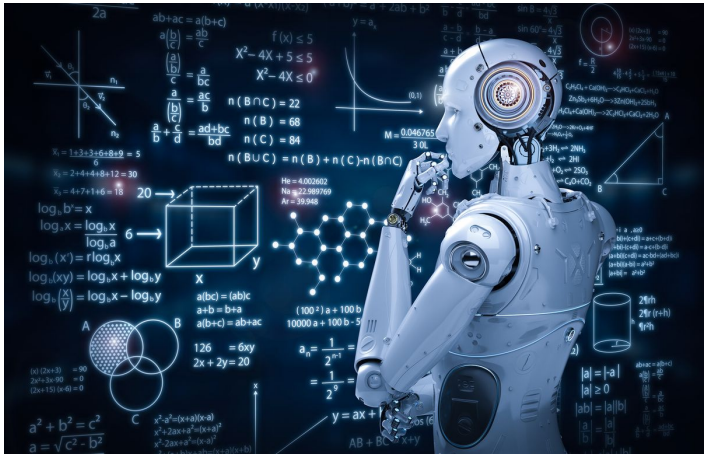
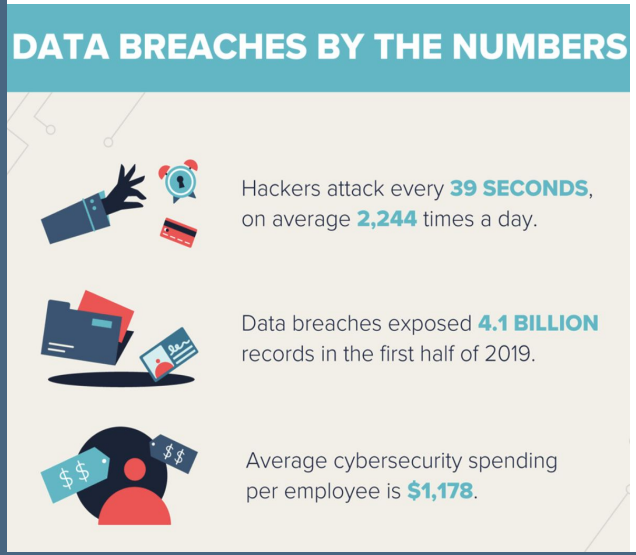
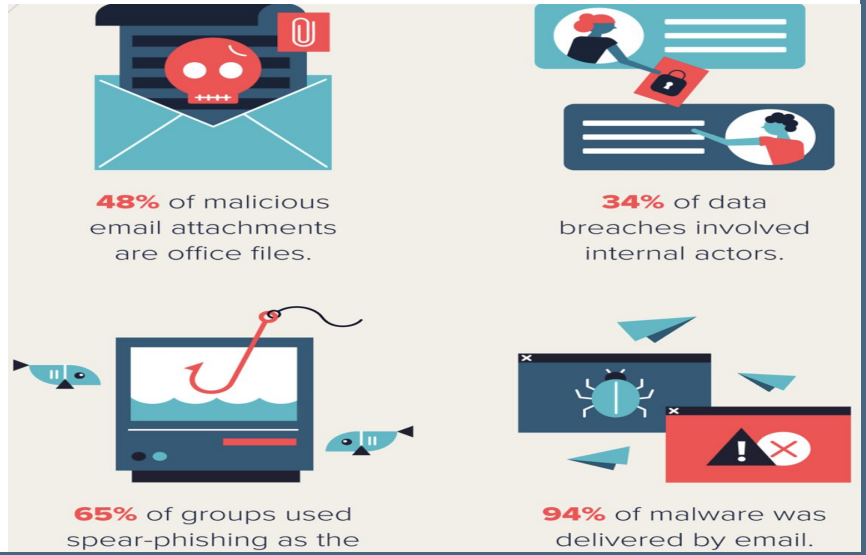


Image Source: Security Info Watch

WHAT IS CYBERSECURITY?

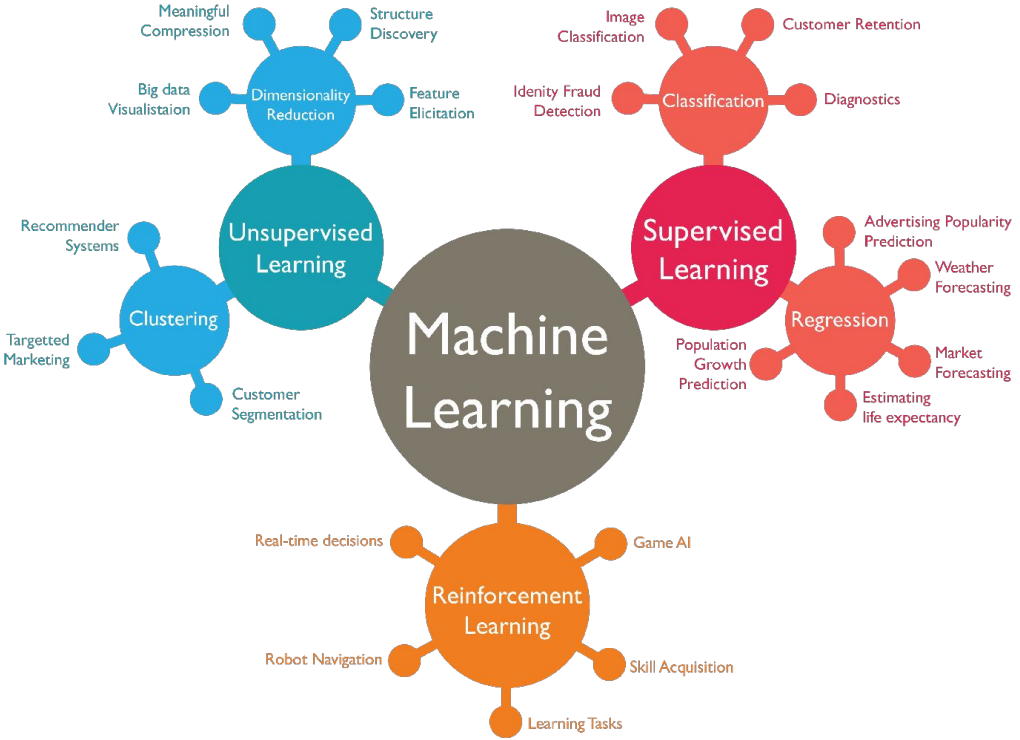
- Cybersecurity is the practice of maintaining confidentiality, integrity and the availability of the data.
- Cybersecurity comprises of set of tools and techniques to protect the data/ information from various attacks.
- Most common types of cyber threats are Malware, Ransomware,Phishing attacks and Social Engineering.
- Companies spend nearly $3.92 millions on data breaches.





WHAT IS MACHINE LEARNING?

- It is an application of artificial intelligence and it provides the ability for the system to automatically without any human intervention and trains the system to take decision with any external programming.
- Machine Learning methods are of 3 types:
  - Supervised learning
  - Unsupervised learning
  - Reinforcement learning



WHAT IS DEEP LEARNING?

- Subset of Machine Learning
- Takeaway features:
  - Scalability
  - Feature Training
- *Deep* refers to the number of layers involved
  - *Deep* Learning versus *Shallow* Learning
- Modeling inspired by the brain -> Artificial Neural Networks

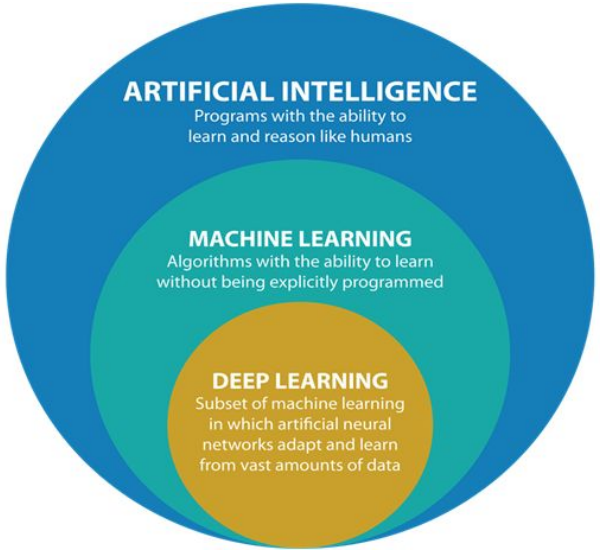


Image Source: Data Catchup

WHAT ARE ARTIFICIAL NEURAL NETWORKS?

- Type of A.I. technology
- Based on how the neurons in the brain works
  - Consists of nodes
  - Input and output with hidden layers in between
- Can generate nonlinear models
- Requires more time and power as the task becomes more complex

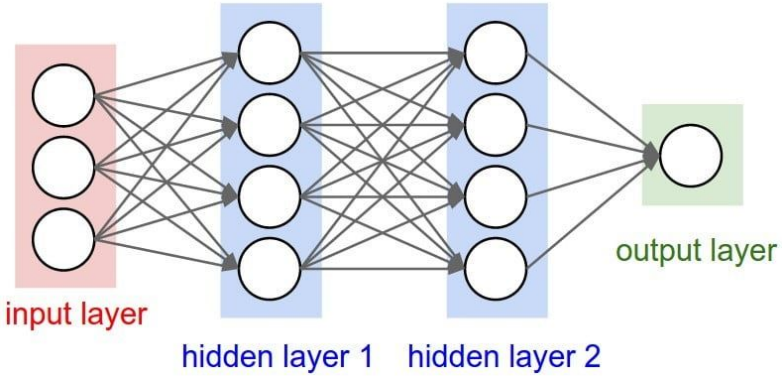


Image Source: digitaltrends

CIA TRIAD


INTEGRITY
CIA
TRIAD
24/7
CONFIDENTIALITY
AVAILABILITY
SPANNING
A Kaseya COMPANY

SECURITY GOAL #1: CONFIDENTIALITY

- Confidentiality means protection of data or resources from unauthorized access.
- The hackers usually perform two types of extractions attacks and they are:
    - Model Extraction Attack: extracts the model parameters by sending queries to the model
    - Model Inversion Attack: attacks are carried out by finding the inputs that provide sensitive information from the training datasets when given as input to the models

SECURITY GOAL #1.1: PRIVACY

- Norton defines *privacy* as the rights to information, regarding its access and usage.
- Includes protection of the DL model itself and the training data
- Consider a HIPAA violation…

Image Source: Mercury News

SECURITY GOAL #2: INTEGRITY

- Ensure that the data has not been tampered or compromised
- Ways to impact integrity
  - Modifying data
  - Unintentionally by using bad data
  - Removing data

Image Source: cybersecurityglossary

SECURITY GOAL #3: AVAILABILITY

- *Availability* is the ability of authorized users to access the system, network, and data at will. Interruption of this freedom is an availability attack.
- Example: Denial-of-Service Attack
- False Positives/Misclassifications in ML models

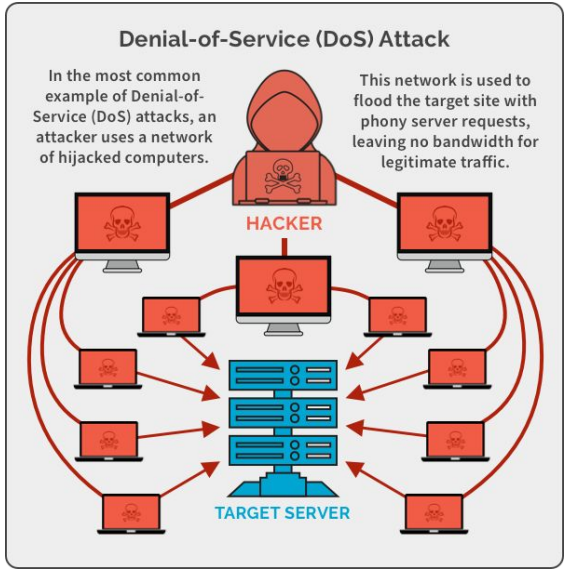


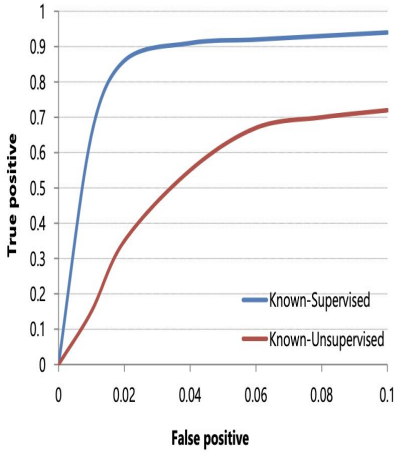
Image Source: Security Boulevard

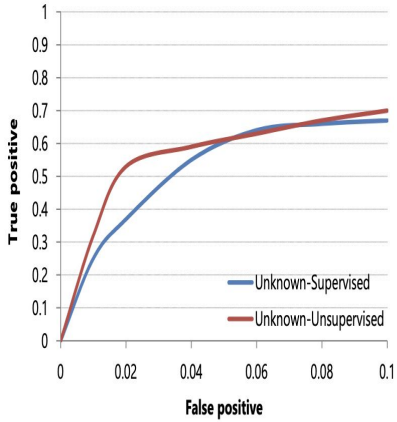
DEEP LEARNING APPLICATIONS IN CYBERSECURITY

- Intrusion Detection/Prevention Systems
- Malware Detection
- Spam/Social Engineering Detection
- Network Traffic Analysis
- User Behavior Analysis

INTRUSION DETECTION/PREVENTION SYSTEMS

- Detect any unusual activity in the system.
- Traditional methods are unable to solve the complex problems
- High false positive and false negative detection rates.
- New techniques with artificial intelligence and computer intelligence were proposed.
- Laskov along with his team members developed an technique that gives 95% accurate results.





MALWARE DETECTION

- "Any type of malicious software designed to harm or exploit any programmable device, service or network."
- Static Analysis versus Dynamic Analysis
- Autoencoders in malware detection applications
  - Li Framework
  - DL4MD Model

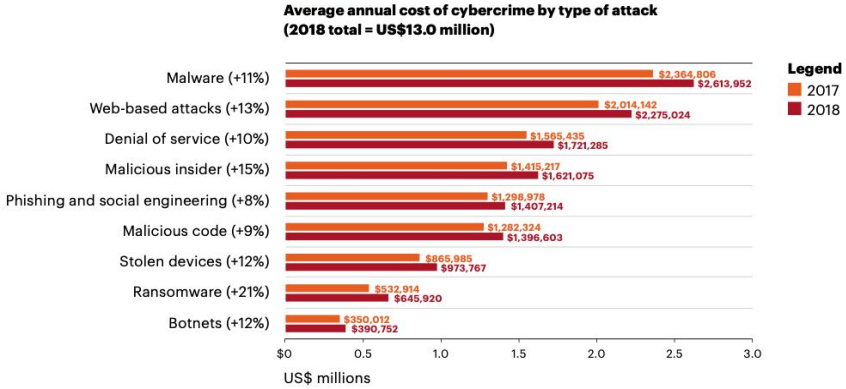
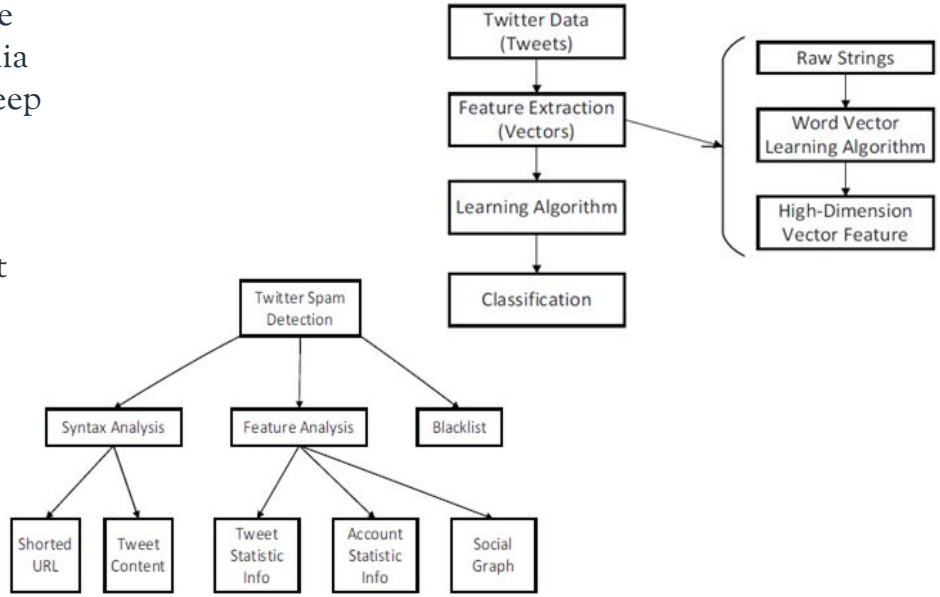


Figure ?: Average annual cost of cybercrime by type of attack, 2018-2019. From *Accenture Ninth Annual Cost of Cybercrime Study*, 2019.

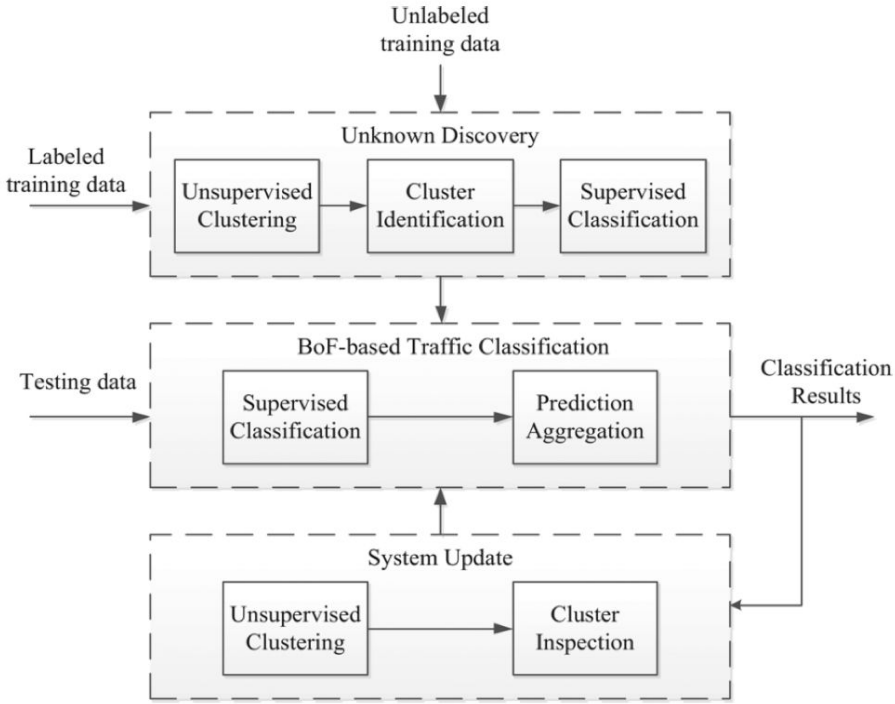
SPAM/SOCIAL ENGINEERING DETECTION

- Detecting spam has become more difficult, especially on social media
- Researchers are starting to use deep learning to detect spam
- Ex: Twitter
- Old method:
  - Characteristic of the tweet
  - Blacklist
  - Time consuming
  - Most would have already visited the site
- New Method:
  - Vectors
  - Deep learning

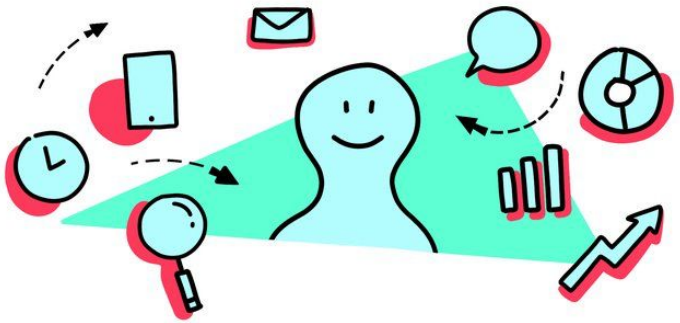


NETWORK TRAFFIC ANALYSIS

- Monitor traffic activity patterns.
- IP address from unusual area is notified.
- Malware behavior is now difficult to detect.
- Especially zero-day attacks are most occuring and have to be prevented.
- A technique to detect the malicious and abnormal behavior was proposed using 3 model framework known as Robust Network Traffic Classification.



USER BEHAVIOR ANALYSIS



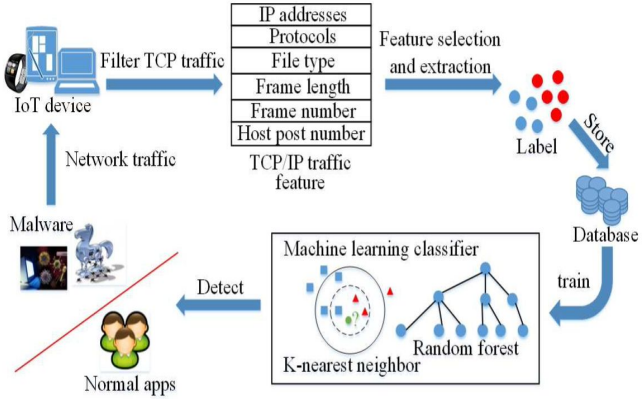
- “Searches for patterns of usage that indicate unusual or anomalous behavior”
- Capable of detecting:
  - Insider threats
  - Targeted attacks
  - Financial fraud
- Recurrent Neural Networks:
  - Tuor model for anomaly detection
  - Fake news detection

USE CASES

- Internet of Things
- Ring Intrusion Detection Devices
- Android Malware Detection

INTERNET OF THINGS (IOT)

- Billions of devices are connected using Internet of Things.
- IoT components are vast and hence the attack surface area is huge and the devices are easily vulnerable.
- Mirai Attack took down thoused of IoT devices.
- Narudin et al. proposed method to detect abnormal behavior in IoT devices.
    - K-NN model
    - Random Forest Model
    - Filtering of network traffic components.



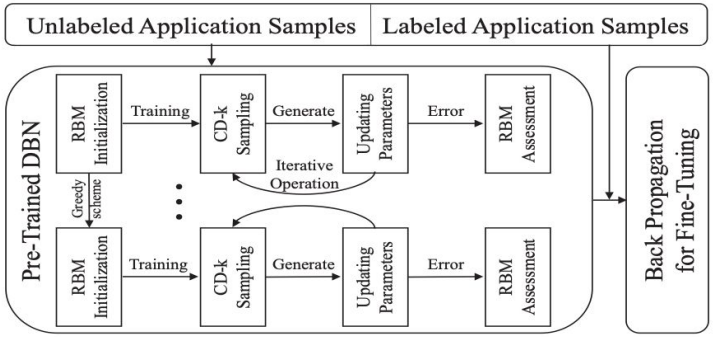
RING INTRUSION DETECTION DEVICES

- There's little research in deep learning for smart devices
- Cameras, smart cars, or voice controlled systems have a vulnerability in IDS
- Ex: Ring
  - There are some cases in which people had their Ring devices hacked.
    - Weak IDS
- To improve IDS in smart devices, adversary attacks are developed
  - To study it
  - To learn to defend against it

Image Source: ring

ANDROID MALWARE DETECTION

- Malware is one of the most common and dangerous threats to a computer system!
- Android, one of the best-selling operating systems worldwide, is even susceptible.
- Yuan et al. DL model for Android Malware Detection
  - Beyond the risk communication technique often adopted
  - Static and Dynamic analysis of 202 features
  - Max. Accuracy of 96.5%
  - DL model outperformed the following ML models: SVM, Naive Bayes, C4.5, Logistic Regression, and Multi-Layer Perceptron



Droid-Sec Framework Model. From *Droid-Sec: Deep Learning in Android Malware Detection*, 2014.

THANK YOU!

QUESTIONS?