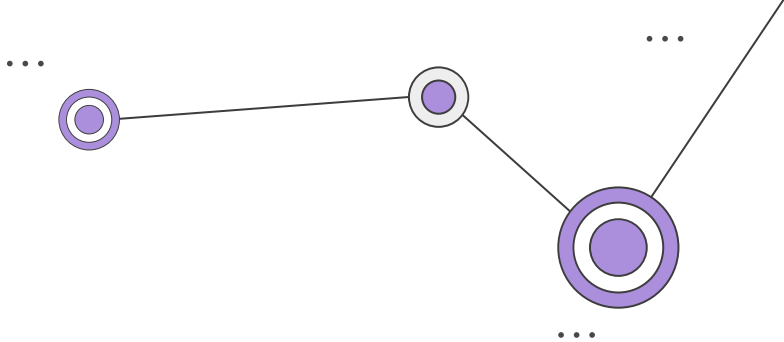


AI Based Intrusion Detection System

Natalia Dai

Clàudia Giró

Mario Martín

Javier Villarreal

TABLE OF CONTENTS

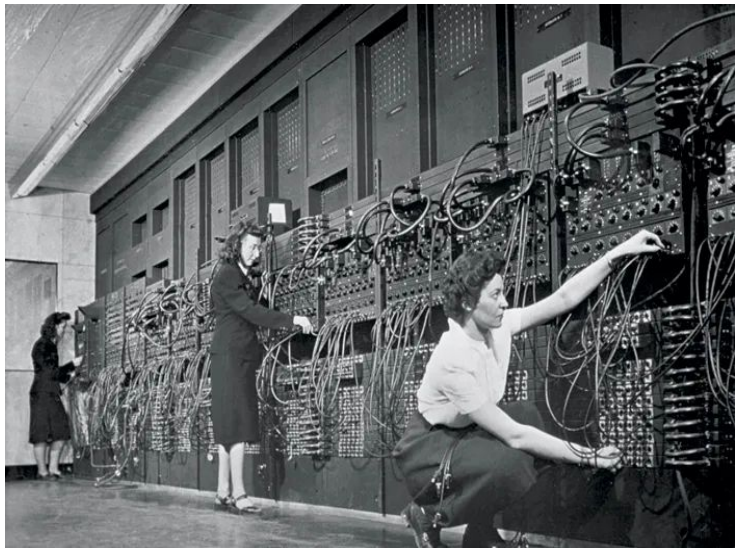
- Evolution of AI
  - Origins
  - Nowadays
- AI Intrusion Detection Systems
  - What is it?
  - How it works
  - Objectives
  - Datasets
  - Types
  - Examples
  - Conclusions

TABLE OF CONTENTS

- **Evolution of AI**
  - **Origins**
  - Nowadays
- AI Intrusion Detection Systems
  - What is it?
  - How it works
  - Objectives
  - Datasets
  - Types
  - Examples
  - Conclusions

Evolution of AI
Origins

- **1940s:**
  - First programmable digital computer
  - Important figures.
  - Binary logic machines.
- **1960s:**
  - *AI Winter.*
- **1970s:**
  - Expert systems.



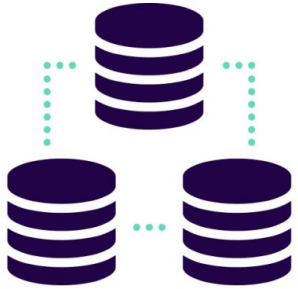
Electronic Numerical Integrator And Computer (ENIAC)

TABLE OF CONTENTS

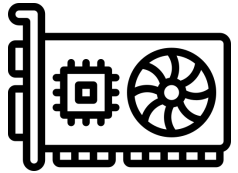
- **Evolution of AI**
  - Origins
  - **Nowadays**
- AI Intrusion Detection Systems
  - What is it?
  - How it works
  - Objectives
  - Datasets
  - Types
  - Examples
  - Conclusions

Evolution of AI
Nowadays

- **2010s:**
  - Resurge of AI technology.
  - *Deep learning*



- **Nowadays:**
  - Present in any aspect of our life.
  - Integrated in every domain.



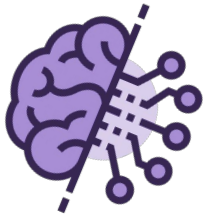
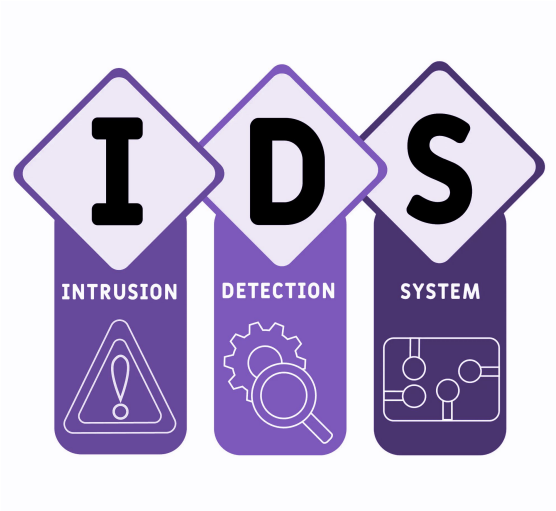


TABLE OF CONTENTS

- Evolution of AI
  - Origins
  - Nowadays
- **AI Intrusion Detection Systems**
  - **What is it?**
  - How it works
  - Objectives
  - Datasets
  - Types
  - Examples
  - Conclusions

AI Intrusion Detection System
What is it?

- Software application or hardware device
- Inspects and monitors the content of network traffic
- Notifies any suspicious activity



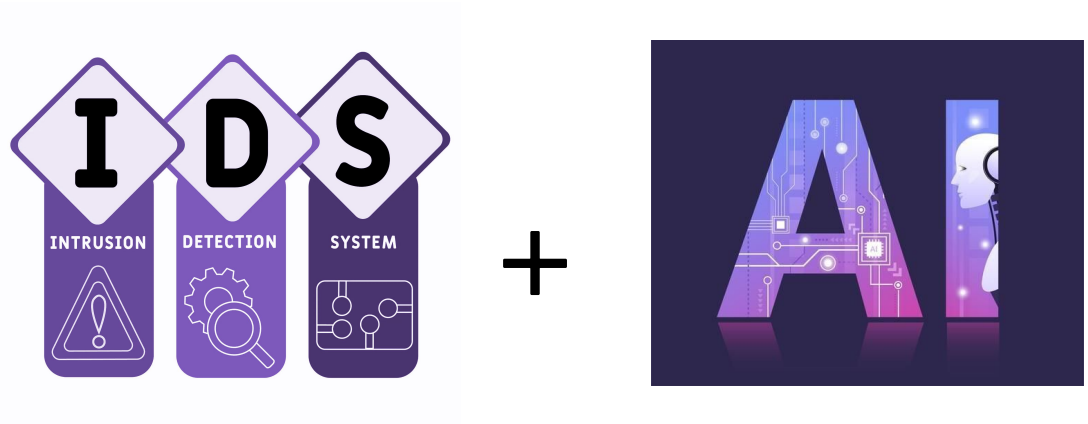
AI Intrusion Detection System

What is it?

- Science of making machines intelligent
- Deep learning algorithms, computer vision, natural language processing and robotics

AI Intrusion Detection System

What is it?



Relies on machine learning algorithms to learn normal network traffic patterns and detect any deviations from them

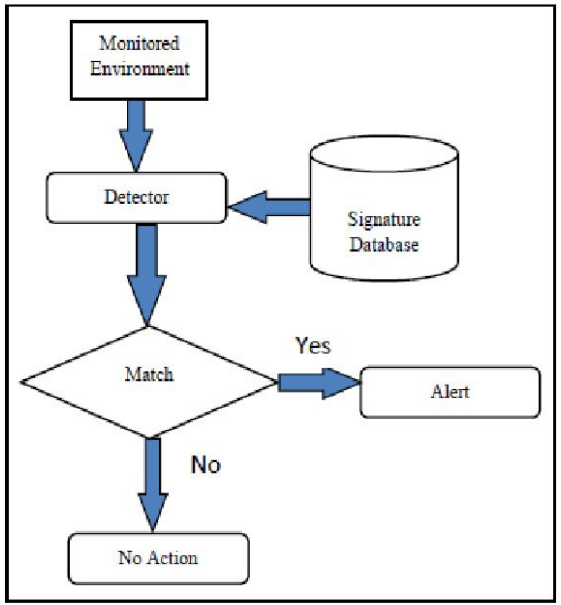
TABLE OF CONTENTS

- Evolution of AI
  - Origins
  - Nowadays
- **AI Intrusion Detection Systems**
  - What is it?
  - **How it works**
  - Objectives
  - Datasets
  - Types
  - Examples
  - Conclusions

AI Intrusion Detection System

How does it work

Signature-based



Anomaly-based

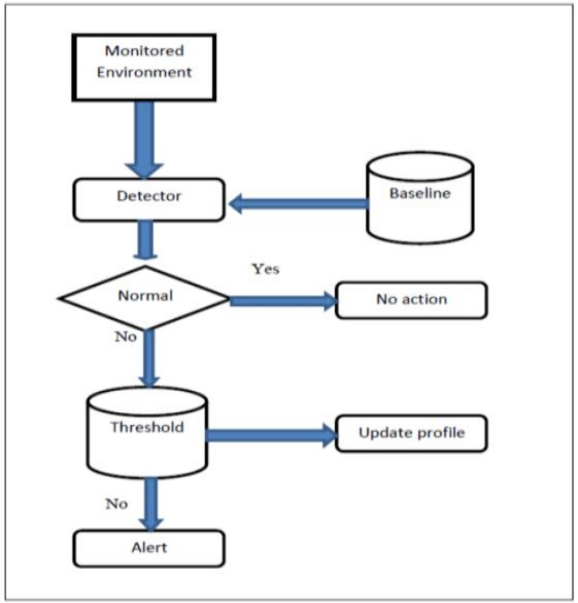


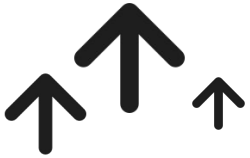
TABLE OF CONTENTS

- Evolution of AI
  - Origins
  - Nowadays
- **AI Intrusion Detection Systems**
  - What is it?
  - How it works
  - **Objectives**
  - Datasets
  - Types
  - Examples
  - Conclusions

AI Intrusion Detection System

Objectives

Improvement of attack detection



Reduce false positives

Detect zero-day attacks

Rapidly adapting

TABLE OF CONTENTS

- Evolution of AI
  - Origins
  - Nowadays
- **AI Intrusion Detection Systems**
  - What is it?
  - How it works
  - Objectives
  - **Datasets**
  - Types
  - Examples
  - Conclusions

AI Intrusion Detection System

Datasets

Data source

Current Datasets

KDDCup99

NSL-KDD

ISCXIDS2012

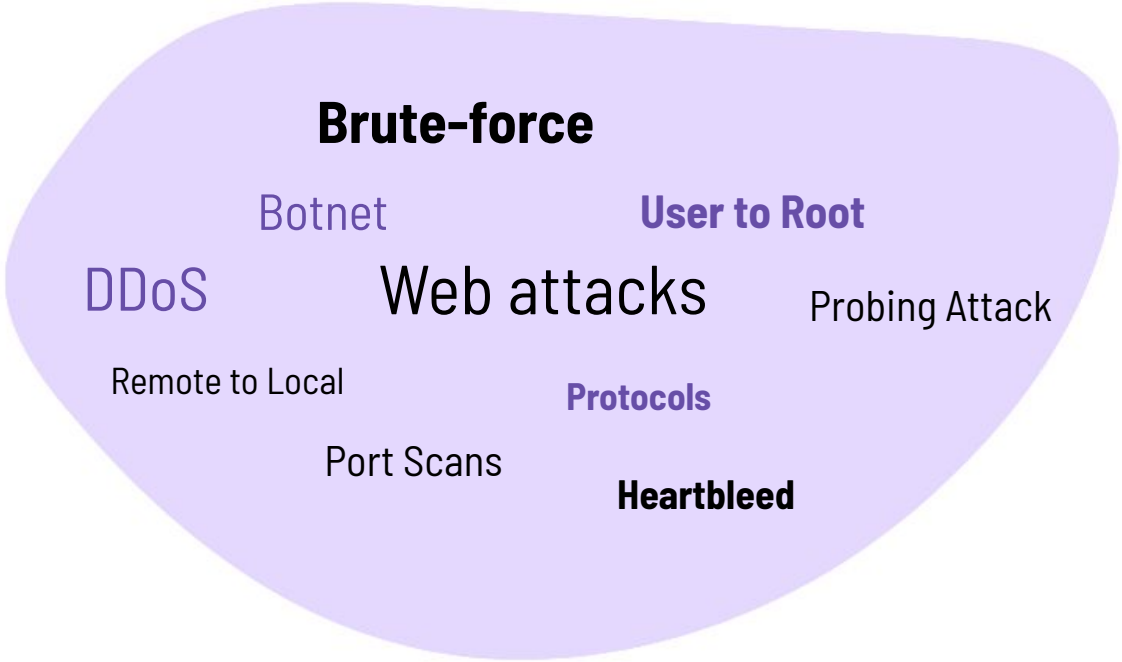
CICIDS2017

CSE-CIC-IDS2018

UNSW-NB15

CIDDS

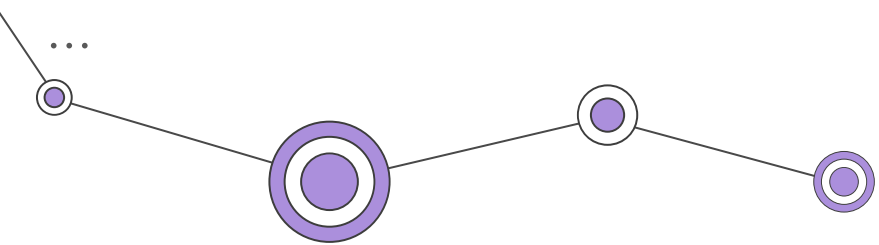
Datasets
Applications



KDDCup99

70%

NSL-KDD



Datasets
Problems

most used ones

but...

- Old traffic
- Do not represent nowadays scenarios
- No real-time properties

TABLE OF CONTENTS

- Evolution of AI
  - Origins
  - Nowadays
- **AI Intrusion Detection Systems**
  - What is it?
  - How it works
  - Objectives
  - Datasets
  - **Types**
  - Examples
  - Conclusions

AI Intrusion Detection System

Types

Machine Learning - based

- Improvement without being programmed.
- Identify patterns...

Deep Learning - based

- Subtype of Machine Learning.
- Uses neural networks to learn from data.

Types
Machine Learning Models

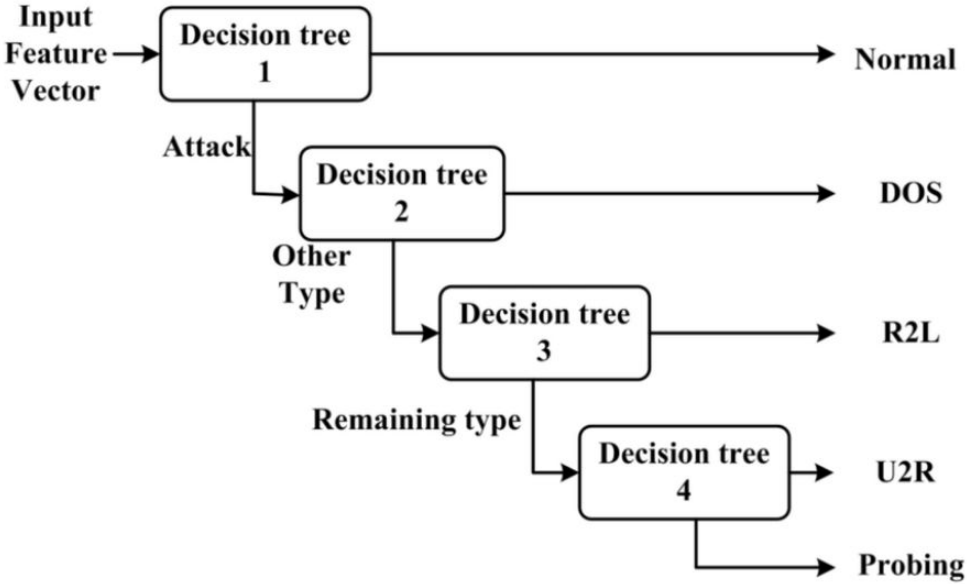
- **Naive Bayes**
- Decision trees
- KNN

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)}$$

Types

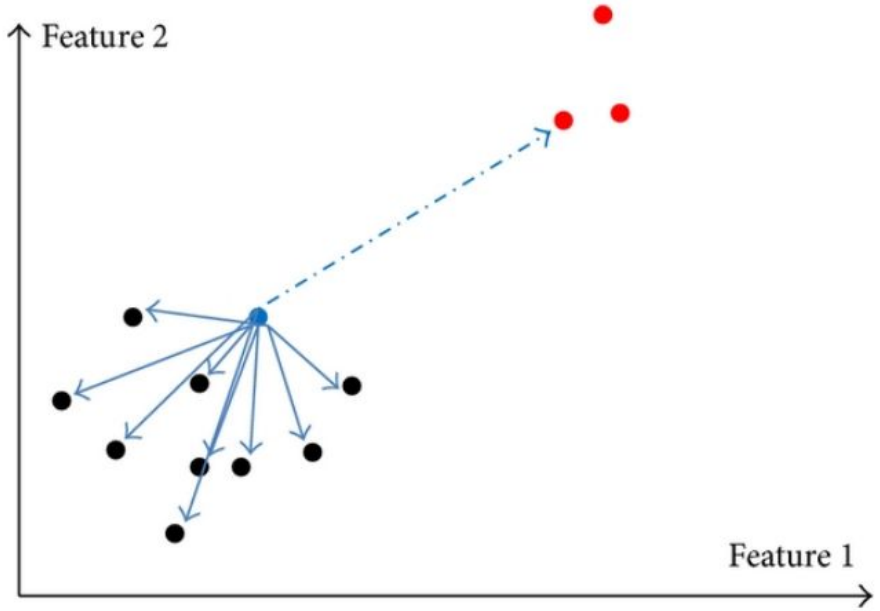
Machine Learning Models

- Naive Bayes
- **Decision trees**
- KNN



Types
Machine Learning Models

- Naive Bayes
- Decision trees
- **KNN**



Types

Deep Learning Models

Artificial Neural Network

- ELM (Extreme Learning Machine)

Convolutional Neural Network

- Two-step preprocessing
- CNN-MCL
- Focus on Kernel Training

Recurrent Neural Network

- UNSW-NB15 with ReLU
- LSTM-RNN
- GRU-RNN

Autoencoders

- SSAE
- Stacked, denoising, nonsymmetric...

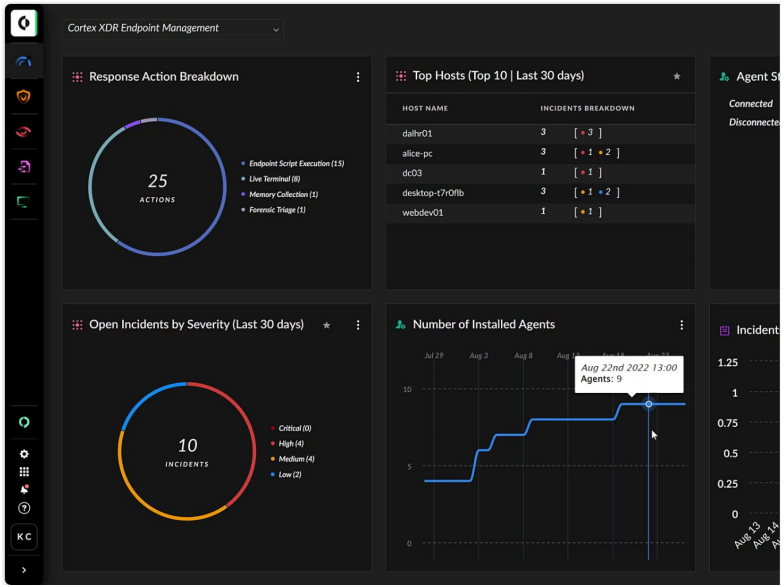
Hybrid methods

TABLE OF CONTENTS

- Evolution of AI
  - Origins
  - Nowadays
- **AI Intrusion Detection Systems**
  - What is it?
  - How it works
  - Objectives
  - Datasets
  - Types
  - **Examples**
  - Conclusions

AI Intrusion Detection System
Examples

- A huge diversity of systems:
  - *Palo Alto Network Cortex XDR*
  - *Deepwatch Deepfence*
  - *Cisco Secure Web Gateway (SWG)*
  - *Microsoft Defender for Cloud*



Cortex XDR user interface

TABLE OF CONTENTS

- Evolution of AI
  - Origins
  - Nowadays
- **AI Intrusion Detection Systems**
  - What is it?
  - How it works
  - Objectives
  - Datasets
  - Types
  - Examples
  - **Conclusions**

AI Intrusion Detection System

Conclusions / Challenges

- Dataset problems
- Hard to compare models
- Lack of different fields (5G, IoT...)
- General lack of investigation