ITU Events

ITU Regional Cybersecurity Forum for Europe and CIS

27 – 28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of infocommunication infrastructure to make cities and human settlements inclusive, safe, and resilient

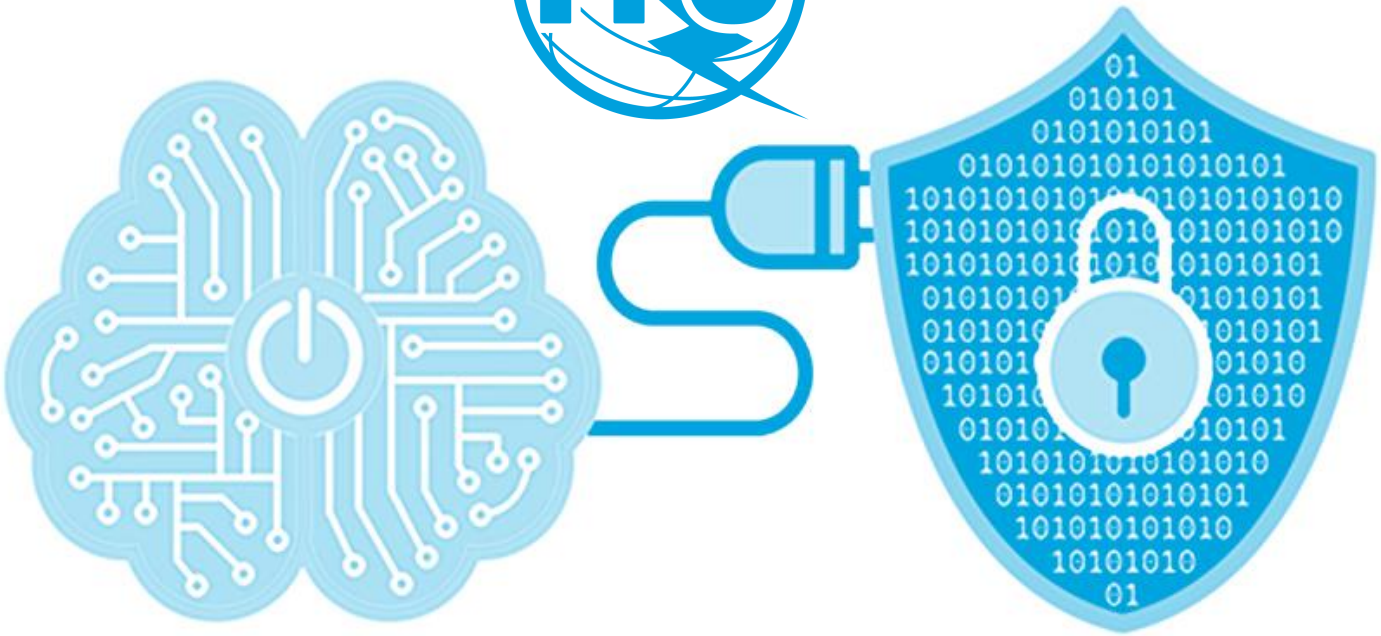
POLICIES & STRATEGIES | CERTIFICATION FRAMEWORKS | DATA PROTECTION | SECURITY CHALLENGES | 5G, eSIM IoT, AI

Hosted and co-organized by:

REPUBLIC OF BULGARIA
State e-Government Agency

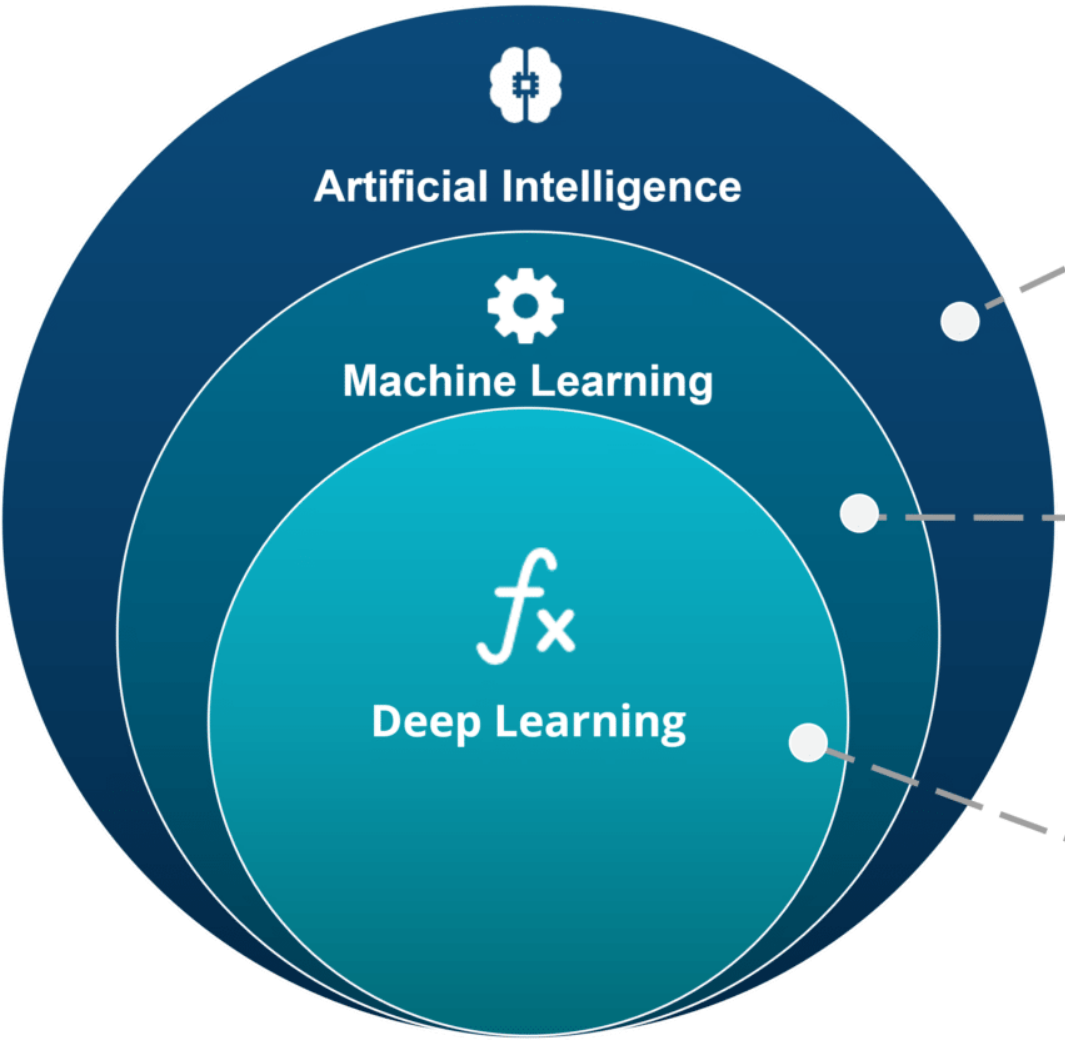
REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

ITU



Applications of Neural Networks in Cybersecurity

Marwan Ben Rached
Technical Officer – Cybersecurity
International Telecommunication Union



ARTIFICIAL INTELLIGENCE

A technique which enables machines to mimic human behaviour

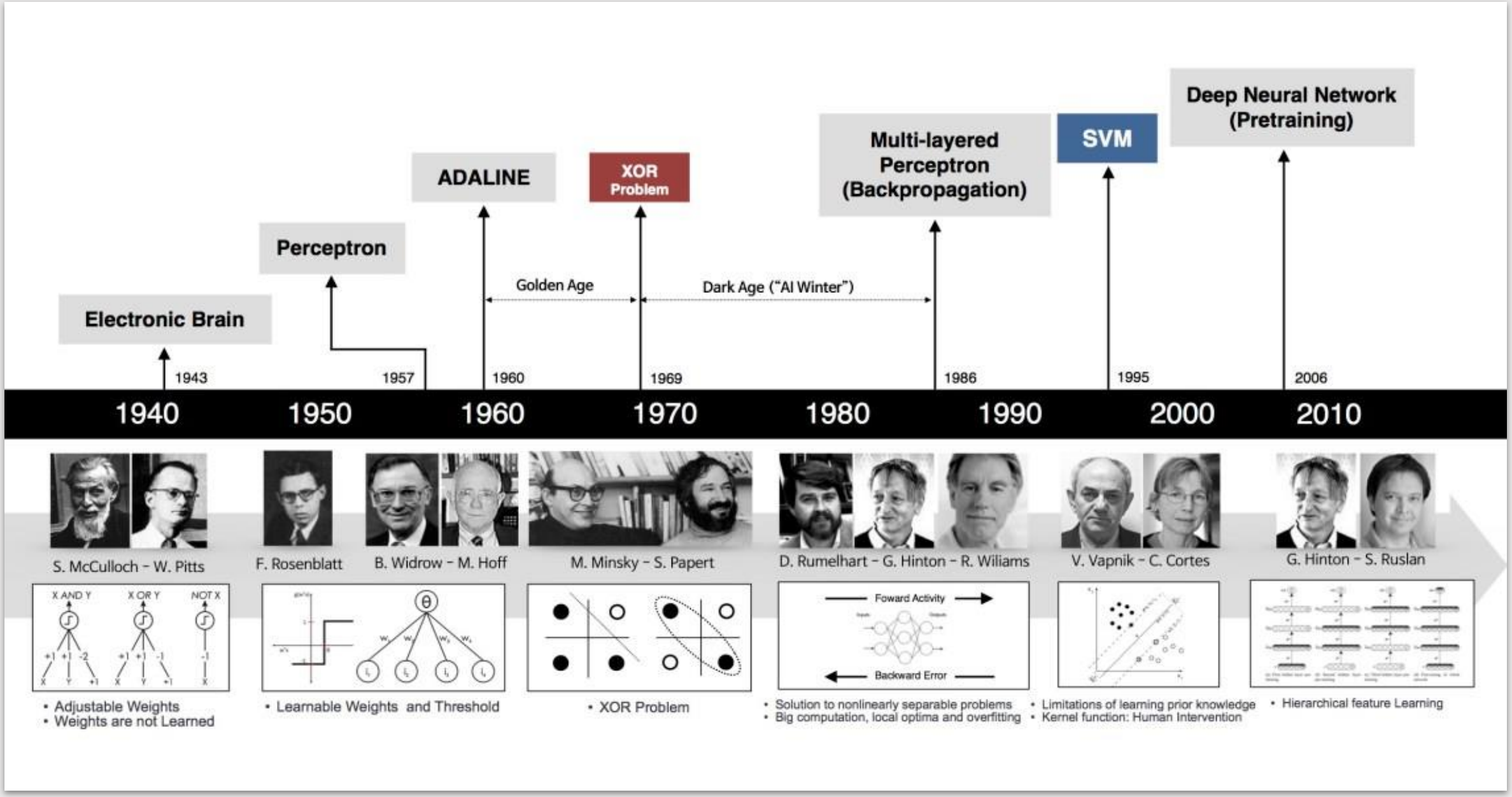
MACHINE LEARNING

Subset of AI technique which use statistical methods to enable machines to improve with experience

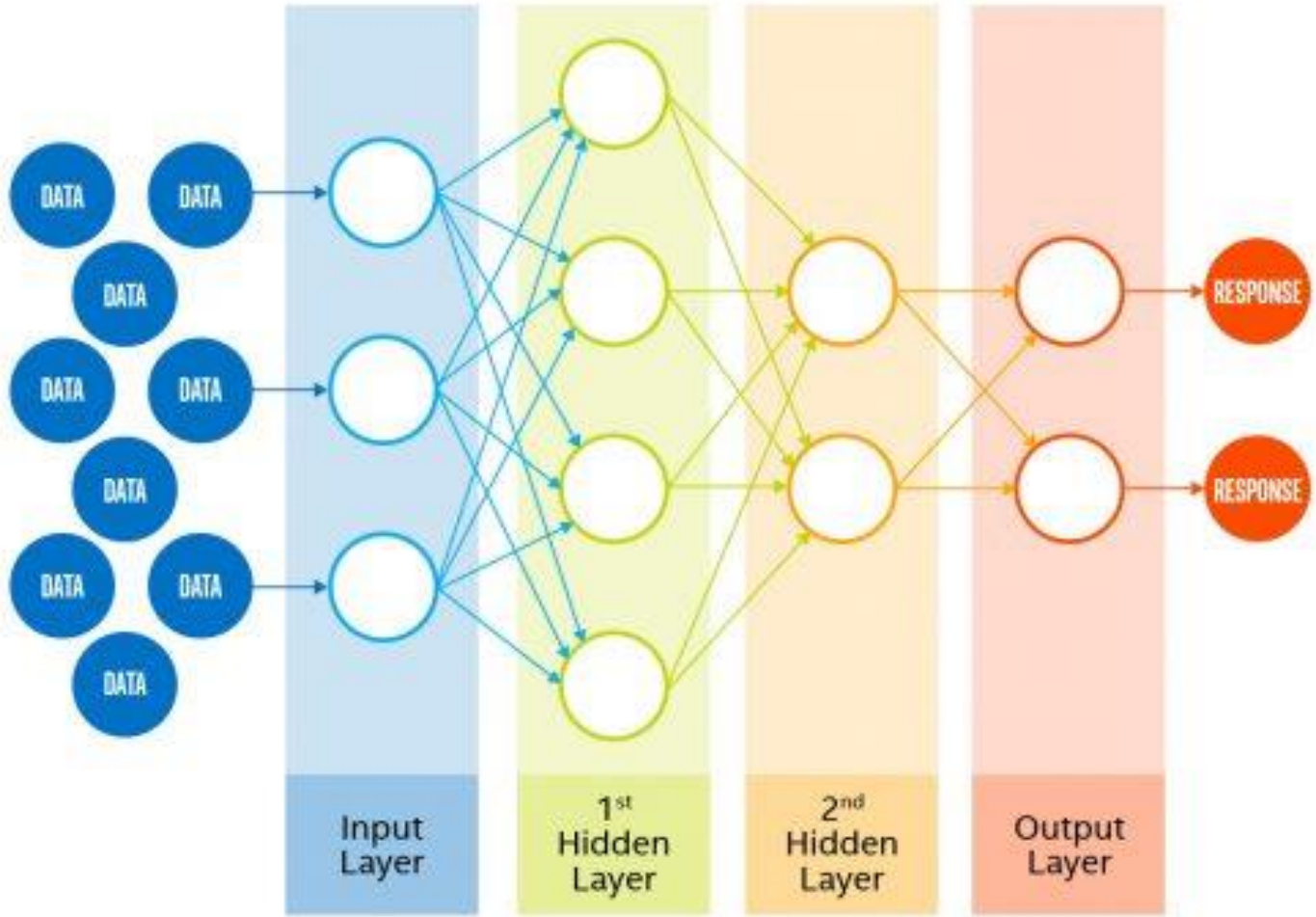
DEEP LEARNING

Subset of ML which make the computation of multi-layer neural network feasible


The Digital Universe is Huge —And Growing Exponentially
4.4 ZB
2013
44 ZB
2020
If the Digital Universe were represented by the memory in a stack of tablets, in 2013 it would have stretched two-thirds the way to the Moon*
By 2020, there would be 6.6 stacks from the Earth to the Moon*
Source: IDC, 2014
* iPad Air – 0.29" thick, 128 GB

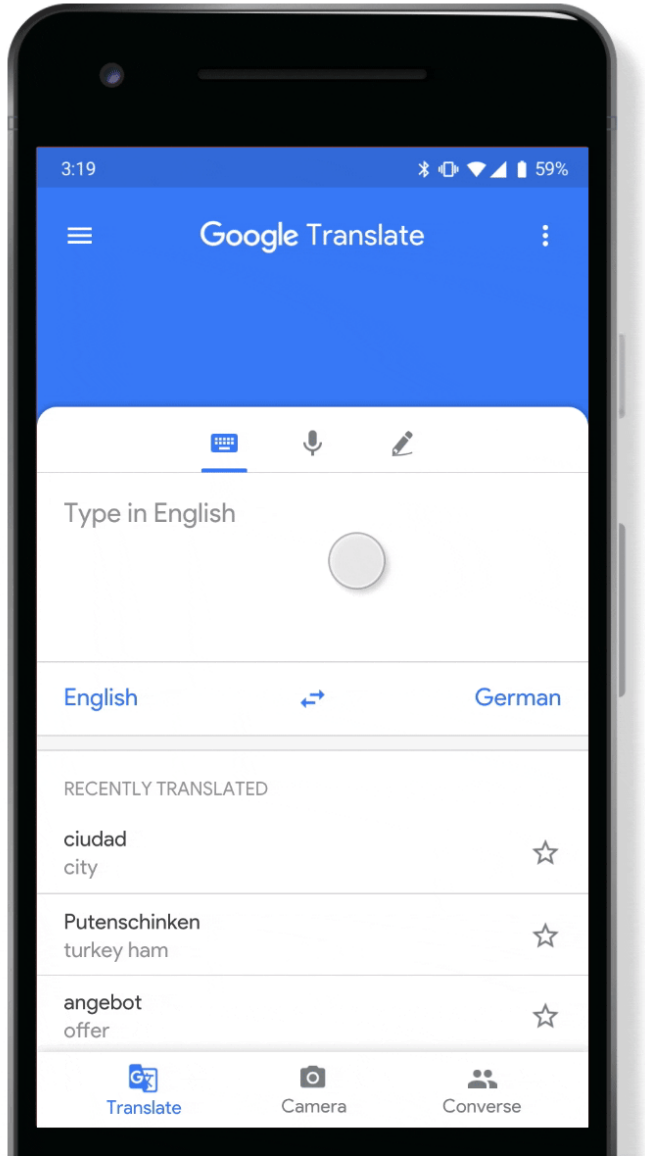

Deep Neural Network
(Pretraining)
SVM
Multi-layered
Perceptron
(Backpropagation)
XOR
Problem
ADALINE
Perceptron
Electronic Brain
Golden Age
Dark Age ("AI Winter")
1943
1957
1960
1969
1986
1995
2006
1940
1950
1960
1970
1980
1990
2000
2010
S. McCulloch - W. Pitts
F. Rosenblatt
B. Widrow - M. Hoff
M. Minsky - S. Papert
D. Rumelhart - G. Hinton - R. Wiliams
V. Vapnik - C. Cortes
G. Hinton - S. Ruslan
X AND Y
X OR Y
NOT X
Foward Activity
Backward Error
• Adjustable Weights
• Weights are not Learned
• Learnable Weights and Threshold
• XOR Problem
• Solution to nonlinearly separable problems
• Big computation, local optima and overfitting
• Limitations of learning prior knowledge
• Kernel function: Human Intervention
• Hierarchical feature Learning

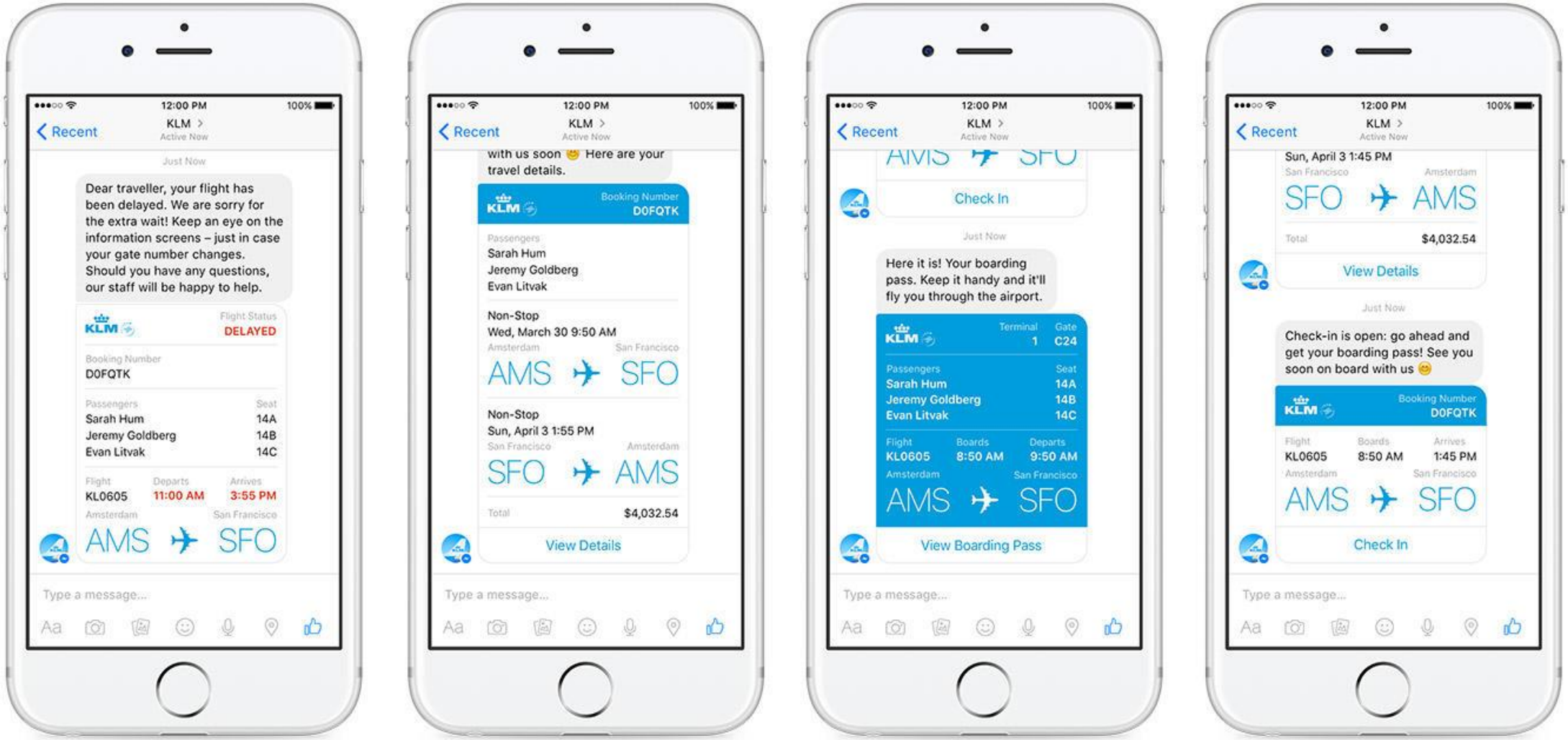
A SIMPLE NEURAL NETWORK




LEFT REARWARD VEHICLE CAMERA
MEDIUM RANGE VEHICLE CAMERA
RIGHT REARWARD VEHICLE CAMERA
MOTION FLOW
LANE LINES
LANE LINES
ROAD FLOW
IN-PATH OBJECTS
ROAD LIGHTS
OBJECTS
ROAD SIGNS


AT&T
1:51 PM
16%
"Hey Siri"
tap to edit
Yo.


3:19
59%
Google Translate
Type in English
English
German
RECENTLY TRANSLATED
ciudad
city
Putenschinken
turkey ham
angebot
offer
Translate
Camera
Converse


12:00 PM
100%
Recent
KLM
Active Now
Just Now
Dear traveller, your flight has been delayed. We are sorry for the extra wait! Keep an eye on the information screens – just in case your gate number changes. Should you have any questions, our staff will be happy to help.
KLM
Flight Status
DELAYED
Booking Number
D0FQTK
Passengers
Seat
Sarah Hum
14A
Jeremy Goldberg
14B
Evan Litvak
14C
Flight
Departs
Arrives
KL0605
11:00 AM
3:55 PM
Amsterdam
San Francisco
AMS
SFO
Type a message...
with us soon Here are your travel details.
Booking Number
D0FQTK
Passengers
Sarah Hum
Jeremy Goldberg
Evan Litvak
Non-Stop
Wed, March 30 9:50 AM
Amsterdam
San Francisco
AMS
SFO
Non-Stop
Sun, April 3 1:55 PM
San Francisco
Amsterdam
SFO
AMS
Total
$4,032.54
View Details
Type a message...
Check In
Just Now
Here it is! Your boarding pass. Keep it handy and it'll fly you through the airport.
KLM
Terminal
Gate
1
C24
Passengers
Seat
Sarah Hum
14A
Jeremy Goldberg
14B
Evan Litvak
14C
Flight
Boards
Departs
KL0605
8:50 AM
9:50 AM
Amsterdam
San Francisco
AMS
SFO
View Boarding Pass
Type a message...
Sun, April 3 1:45 PM
San Francisco
Amsterdam
SFO
AMS
Total
$4,032.54
View Details
Just Now
Check-in is open: go ahead and get your boarding pass! See you soon on board with us
KLM
Booking Number
D0FQTK
Flight
Boards
Arrives
KL0605
8:50 AM
1:45 PM
Amsterdam
San Francisco
AMS
SFO
Check In
Type a message...

Exam: OB
Clipboard: 7/127.85 MB

Voluson™ E10

g, *

E69766-18-09-07-1 GA=20w5d

TIs 0.2
TIb 0.2
MI 0.9

09/07/2018
12:54:14 PM
RM6C

73Hz/ 9.8cm
42°/0.9.
Routine 2 Trim./OB
HI M 7.70 - 4.30-
Gn 0
C7/M7-
P4/E2
SRI II 3-

Voluson
E 10

A B C

V = 0.684 lit
Vol.Angle

Calculating...

SonoCNS

Make sure the Transthalamic plane (TT) is visible in the A-plane area, adjust if needed.

Then press **Start Alignment**

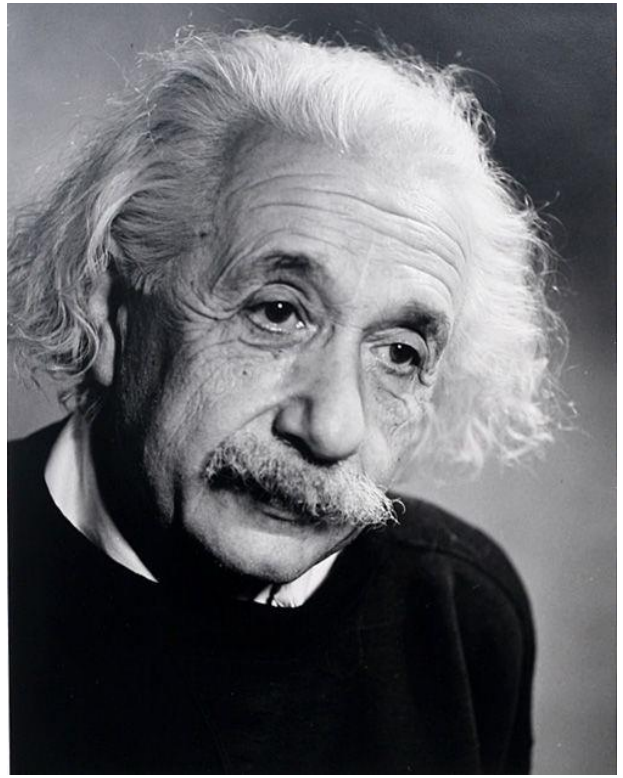
Scan the QR code below with your mobile device to access the ISUOG Guidelines.

No Exam History available

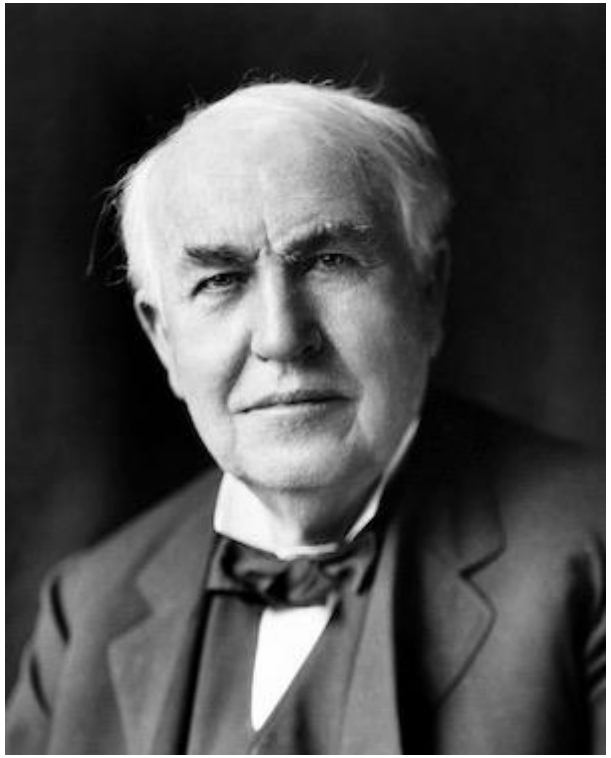
P5
P3 Img
P1 3D
P6
P4
P2 3D

Page 1/1


Profile
Analysis
Sex: M
Race: Hispanic
Age: 34
Weight: 206 lbs

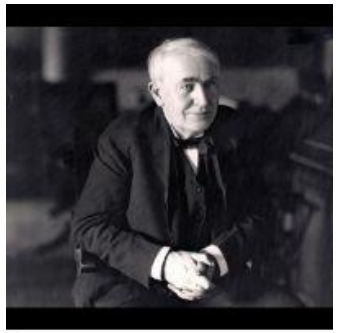
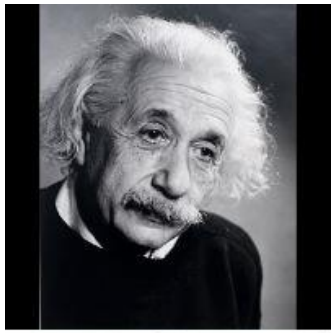


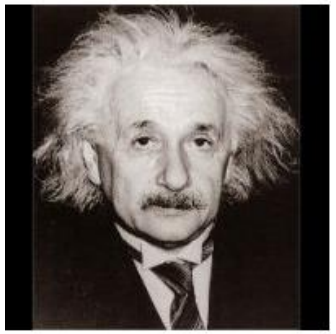
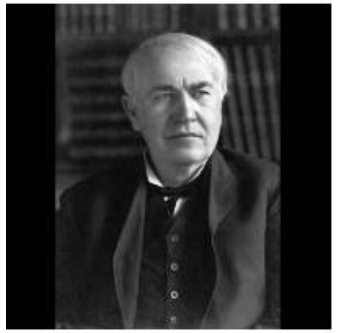
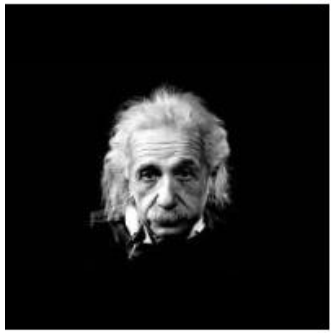
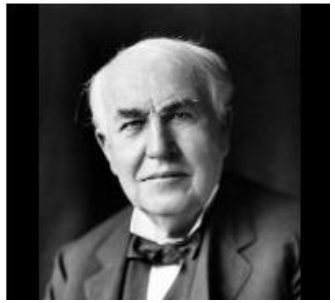
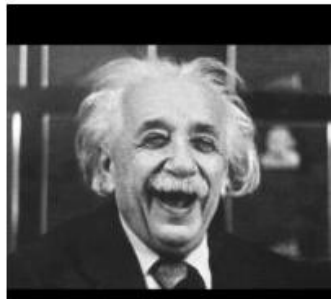
Albert Einstein



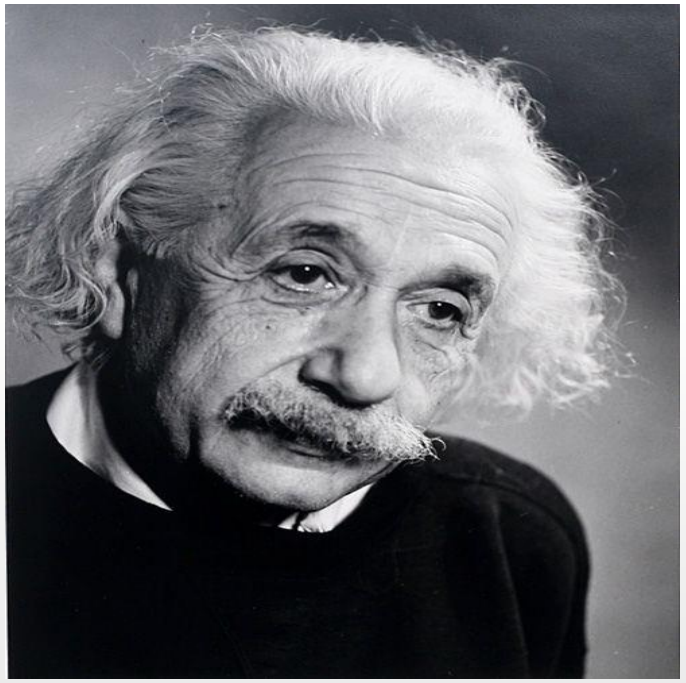
Thomas Edison

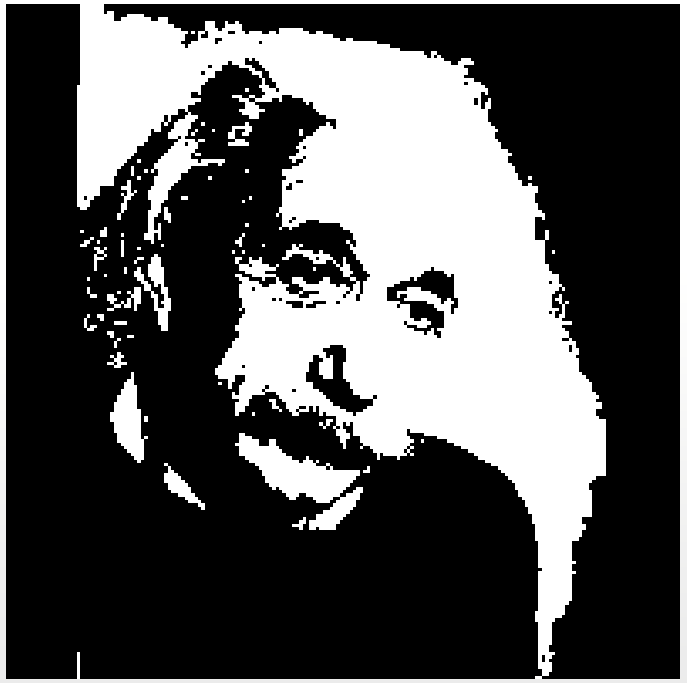
Learning Database

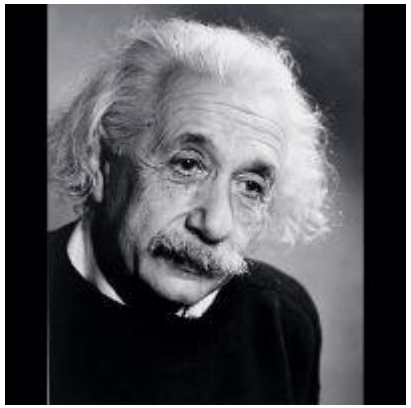
Data Preprocessing



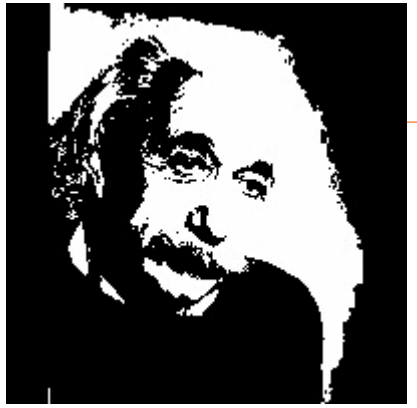


```
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 1 0 1 1 1 0 0 0 0 0 0
0 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0
0 0 0 0 0 1 1 1 1 1 1 1 0 0 0 0
0 0 0 0 0 0 0 0 1 0 1 1 0 0 0 0
0 0 0 0 0 0 1 0 1 1 1 1 1 0 0 0
0 0 0 0 0 1 0 1 1 1 1 1 1 0 0 0
0 0 0 0 1 0 0 0 1 1 1 1 1 0 0 0
0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0
0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0
0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0
0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0
0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

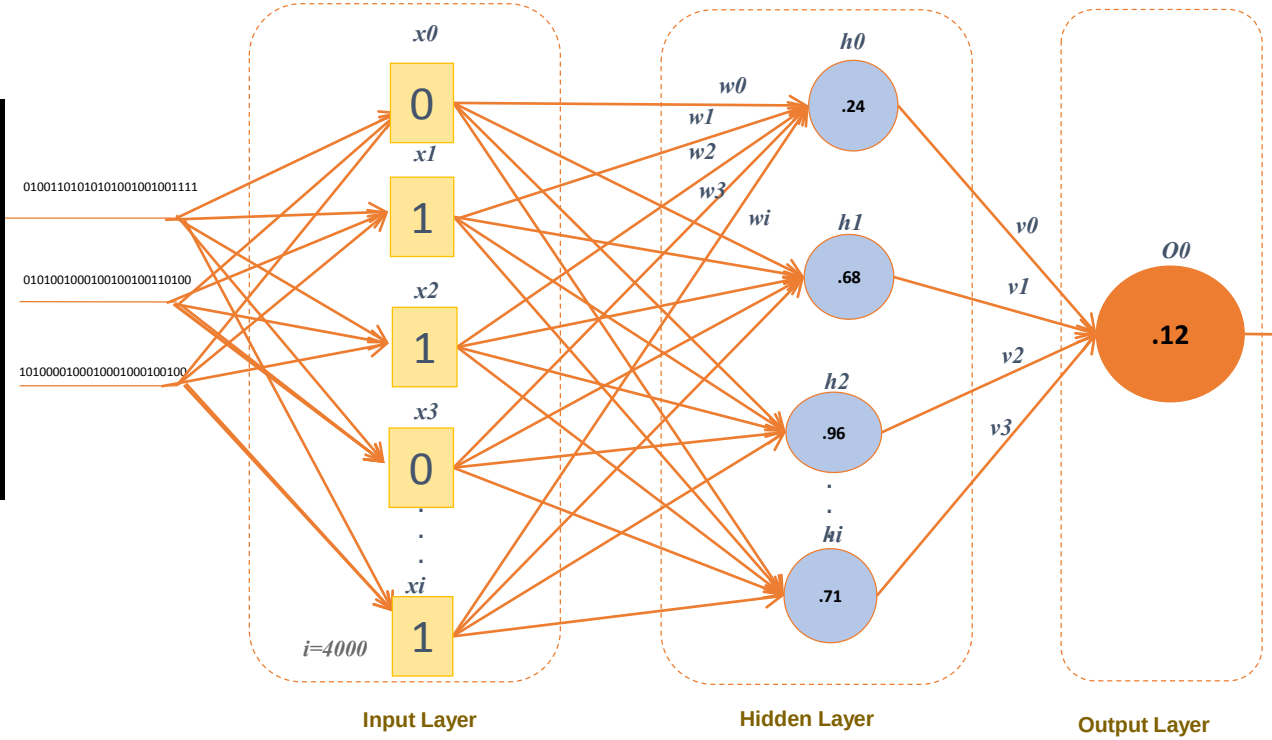
Training phase



200 x 200

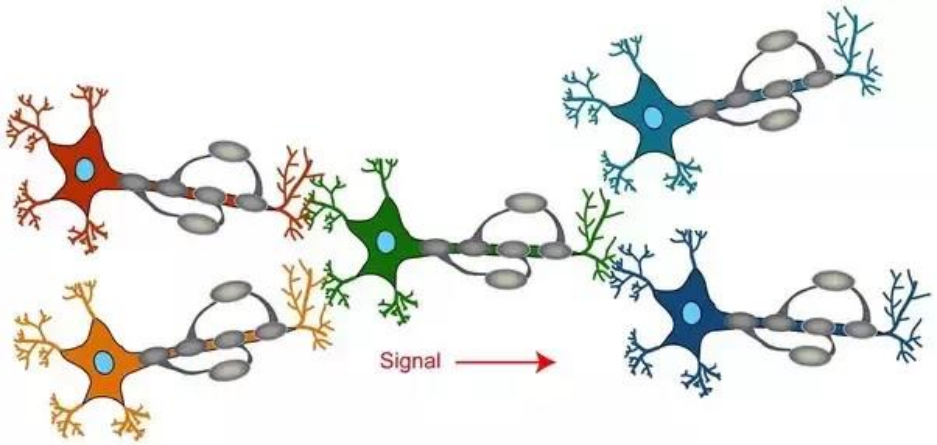


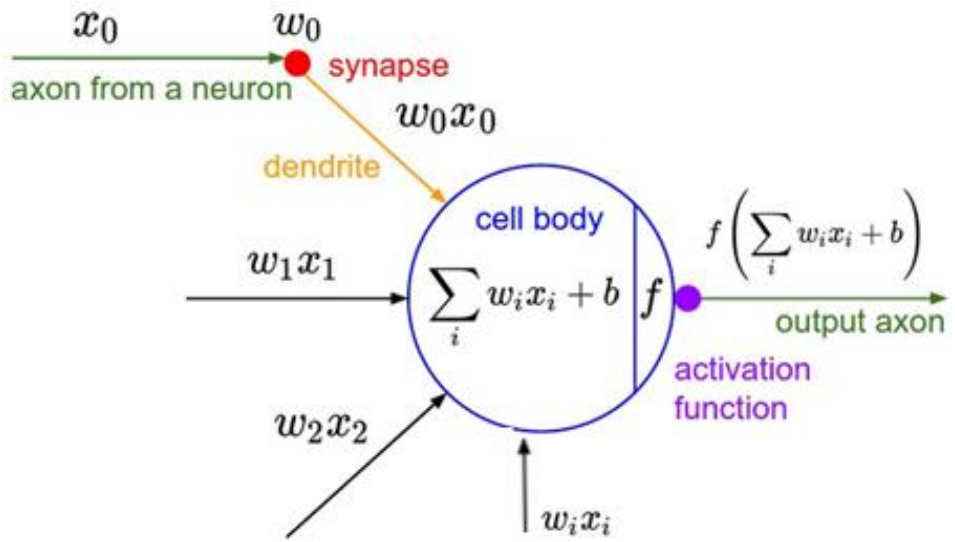
200 x 200



Albert Einstein

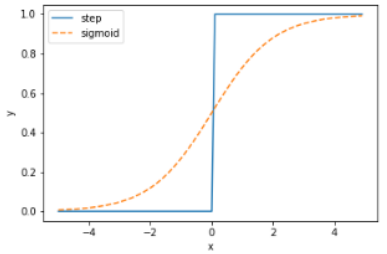
Threshold is 0.5





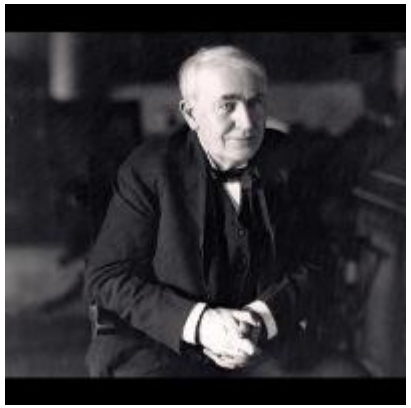
$$z = \sum w_i x_i$$

$$\sigma(z) = \frac{1}{1 + e^{-z}}$$



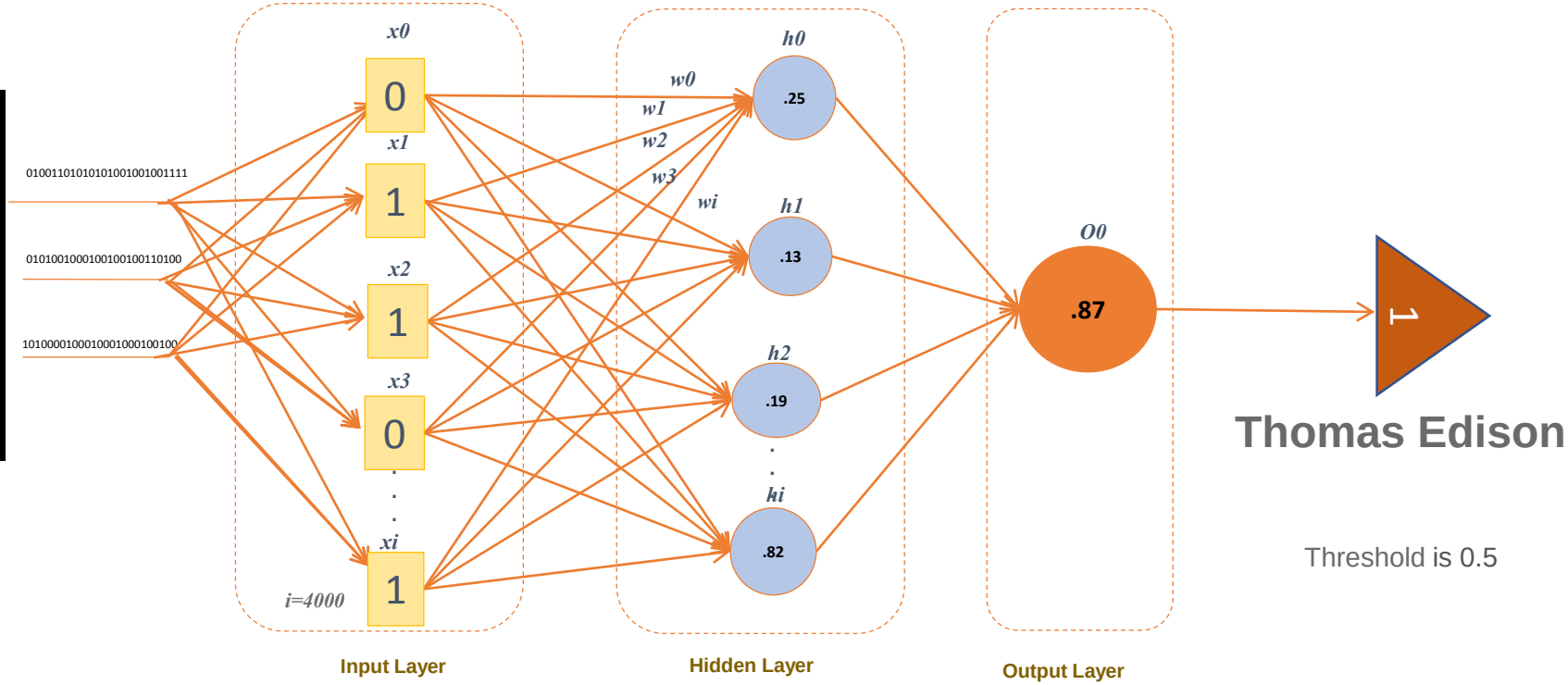
$$E_i = z_i(1 - v_i)(0_0 - v_i)$$

Training phase



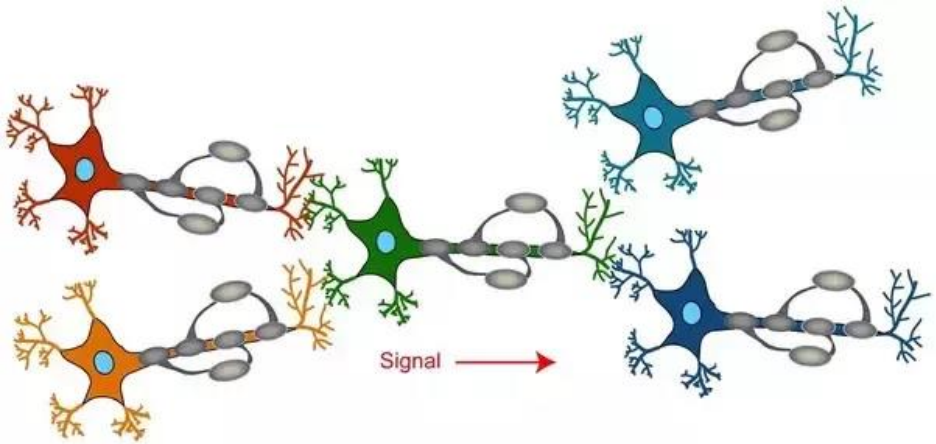
200 x 200

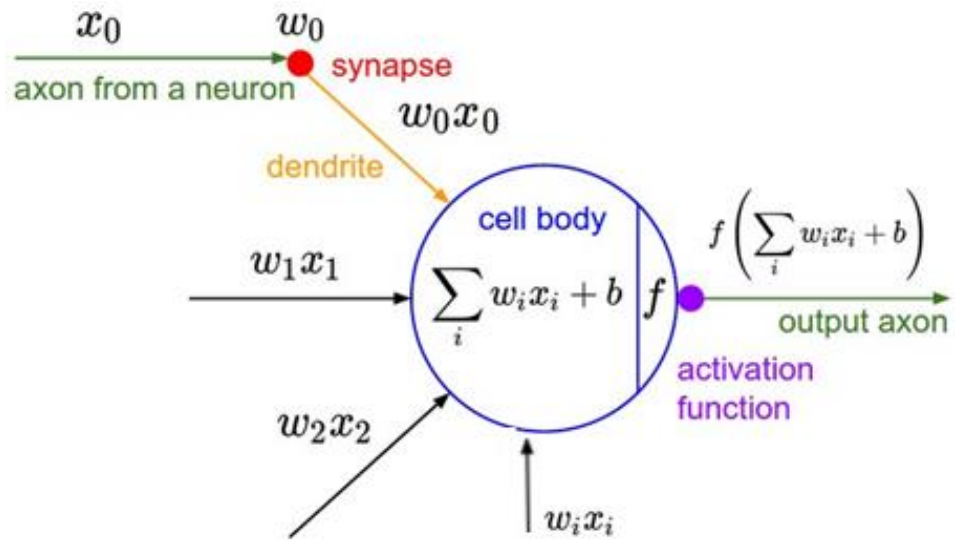
200 x 200



Thomas Edison

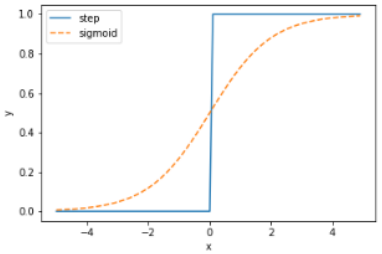
Threshold is 0.5

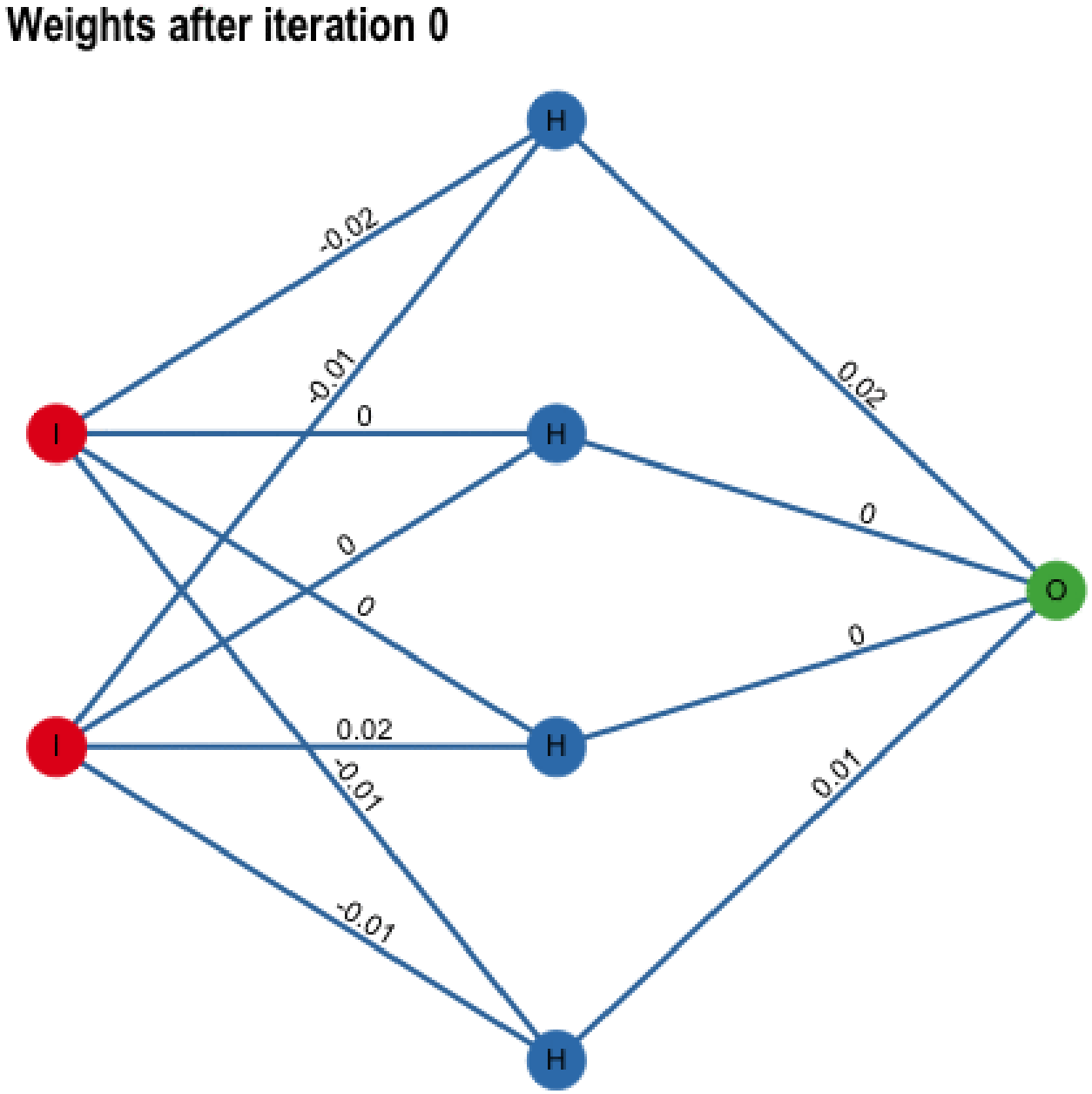




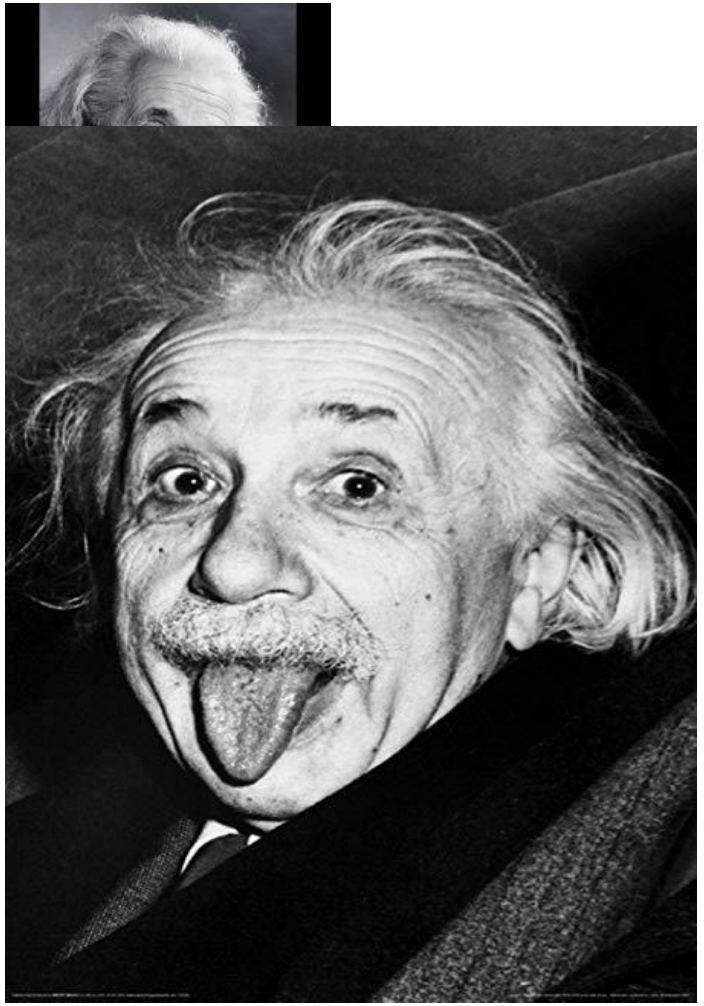
$$z = \sum w_i x_i$$

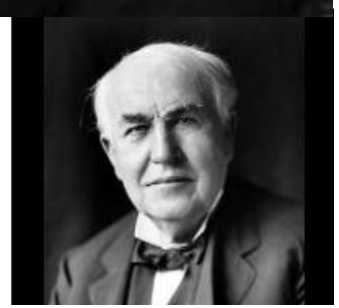
$$\sigma(z) = \frac{1}{1 + e^{-z}}$$

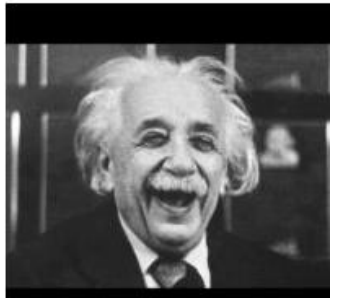


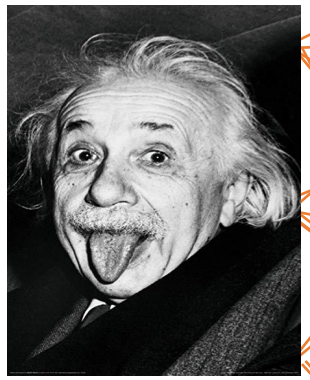

Weights after iteration 0
H
-0.02
-0.01
0.02
I
0
H
0
0
0
O
0
I
0.02
H
-0.01
0.01
-0.01
H

TEST phase









1

0

x2

1

x3

0

xi

0

i=4000

w0

w1

w2

w3

wi

.85

h1

.68

h2

.25

hi

.47

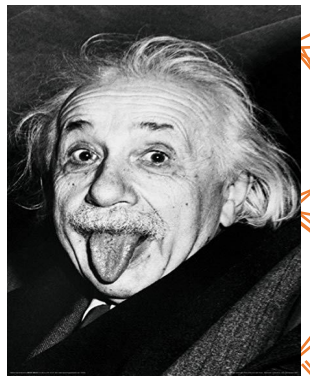
O0

.34

0

Albert Einstein

Threshold is 0.5



1

0

x2

1

x3

0

xi

0

i=4000

w0

w1

w2

w3

wi

.85

h1

.68

h2

.25

hi

.47

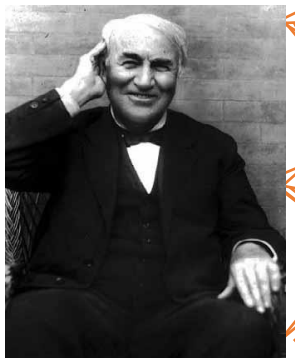
O0

.34

0

Albert Einstein

Threshold is 0.5



1

0

x2

1

x3

0

xi

0

i=4000

w0

w1

w2

w3

wi

.85

h1

.68

h2

.25

hi

.47

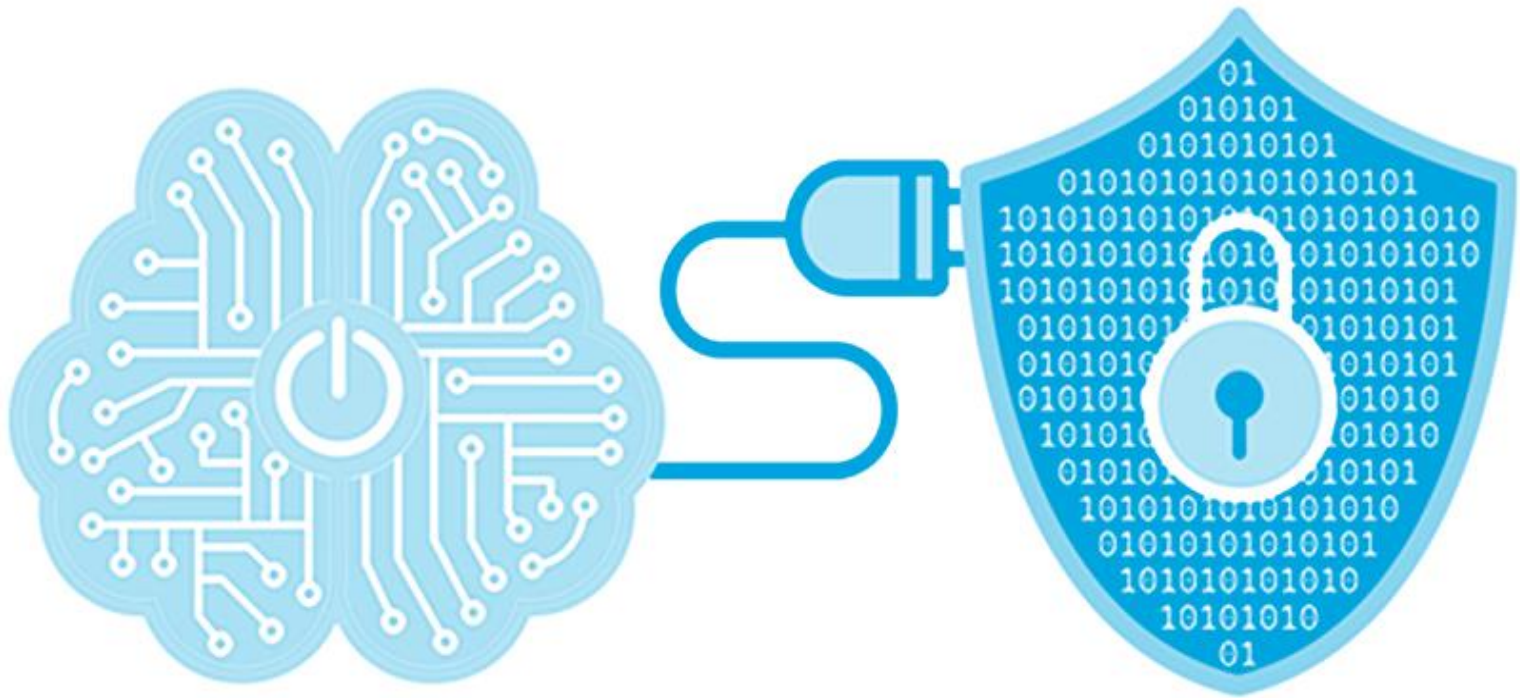
O0

.86

1

Thomas Edison

Threshold is 0.5


01
010101
0101010101
01010101010101010101
1010101010101010101010
1010101010101010101010
1010101010101010101010
01010101 01010101
01010101 01010101
010101 01010
101010 01010
010101 010101
1010101010101010
01010101010101
101010101010
10101010
01

Intelligent Intrusion Detection Systems

Phishing Websites Detection

SPAM Detection

User Behavior Analytics (UBA)

Automated Software Vulnerability Detection

Next Generation Firewall

Next-Generation Antivirus (NGAV)

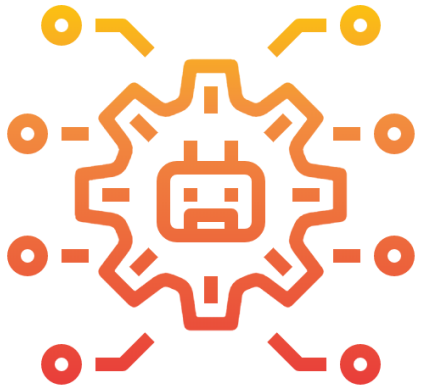
Malware Detection and Classification

Malware Detection and Classification

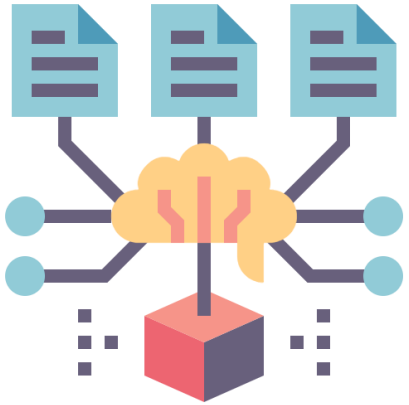
Training phase

Malicious Executables

Benign Executables



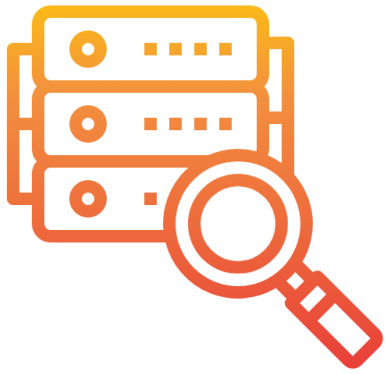
Training



Predictive model

Protection phase

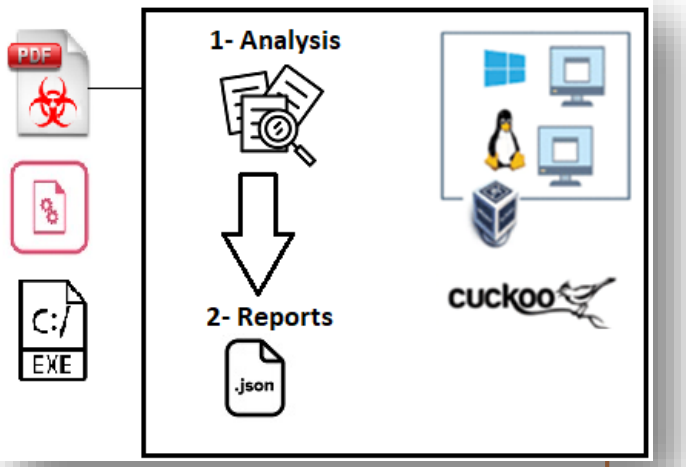
Unknown Executable



Benign / Malicious

Model decision

Malware Detection and Classification



Automated Static File Analysis

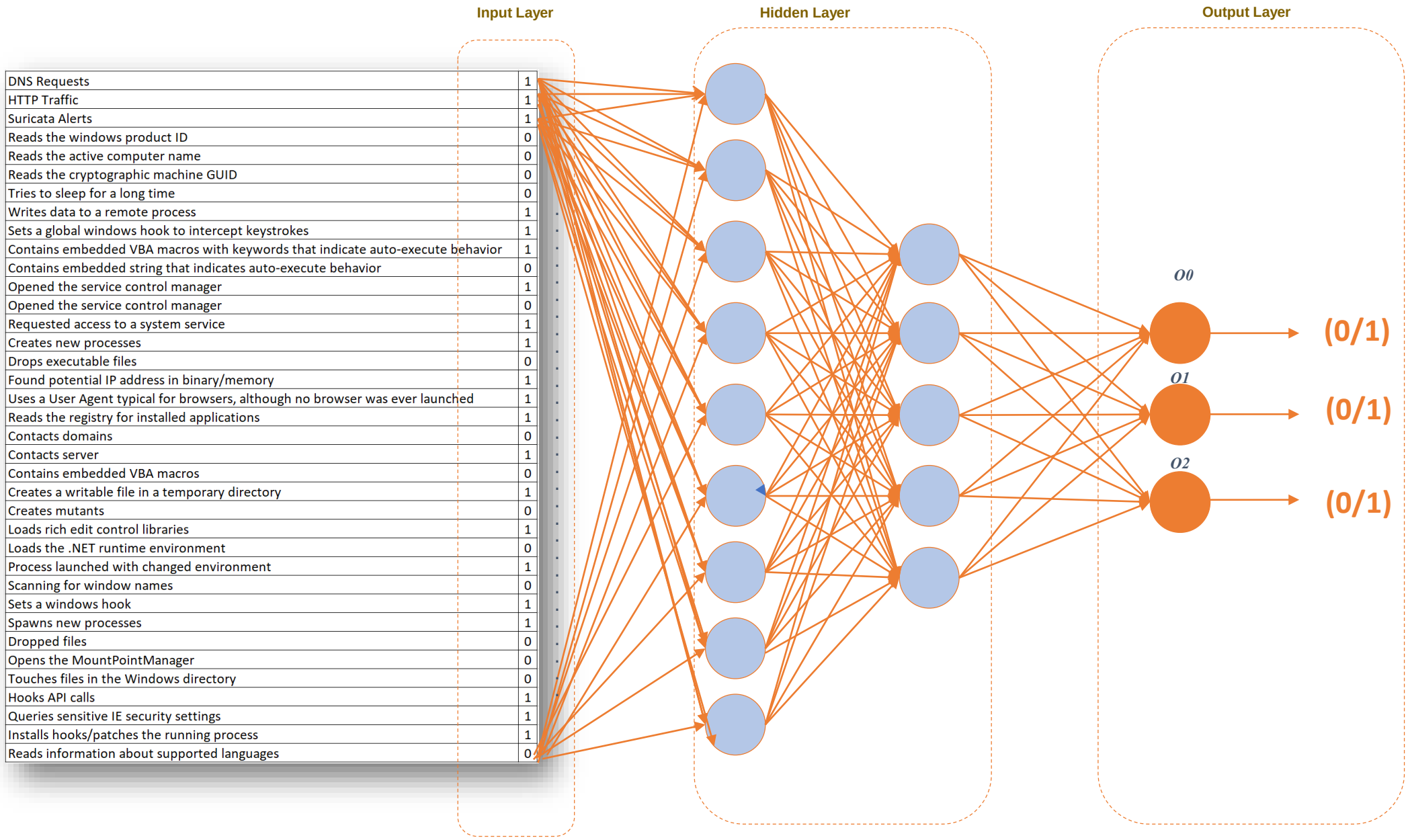

```
...
"hosts": ["0.0.0.0", "255.255.255.255",
"10.0.2.2", "10.0.2.15", "239.255.255.250",
"224.0.0.22", "10.0.2.255"], "dns": [],
"tcp": []}, "behavior": {"processes":
[{"parent_id": "428", "process_name":
"0a1cc307ed378bc79bc524497282c4d9c535cc3014d
8e2a9e72c0baad681b3e9", "process_id": "700",
"first_seen": "20140831184558.308", "calls":
[{"category": "filesystem", "status":
"SUCCESS", "return": "0x00000024",
"timestamp": "20140831184558.308",
"repeated": 0, "api": "CreateFileW",
"arguments": [{"name": "lpFileName",
"value": "C:\\WINDOWS\\system32
\\duser.dll"}, {"name": "dwDesiredAccess",
"value": "GENERIC_READ"}]}, {"category":
"filesystem", "status": "SUCCESS", "return":
"", "timestamp": "20140831184558.308",
...
```


Analysis Report

DNS Requests	1
HTTP Traffic	1
Suricata Alerts	1
Reads the windows product ID	0
Reads the active computer name	0
Reads the cryptographic machine GUID	0
Tries to sleep for a long time	0
Writes data to a remote process	1
Sets a global windows hook to intercept keystrokes	1
Contains embedded VBA macros with keywords that indicate auto-execute behavior	1
Contains embedded string that indicates auto-execute behavior	0
Opened the service control manager	1
Opened the service control manager	0
Requested access to a system service	1
Creates new processes	1
Drops executable files	0
Found potential IP address in binary/memory	1
Uses a User Agent typical for browsers, although no browser was ever launched	1
Reads the registry for installed applications	1
Contacts domains	0
Contacts server	1
Contains embedded VBA macros	0
Creates a writable file in a temporary directory	1
Creates mutants	0
Loads rich edit control libraries	1
Loads the .NET runtime environment	0
Process launched with changed environment	1
Scanning for window names	0
Sets a windows hook	1
Spawns new processes	1
Dropped files	0
Opens the MountPointManager	0
Touches files in the Windows directory	0
Hooks API calls	1
Queries sensitive IE security settings	1
Installs hooks/patches the running process	1
Reads information about supported languages	0

Behavioral Patterns

Malware Detection and Classification



DNS Requests	1
HTTP Traffic	1
Suricata Alerts	1
Reads the windows product ID	0
Reads the active computer name	0
Reads the cryptographic machine GUID	0
Tries to sleep for a long time	0
Writes data to a remote process	1
Sets a global windows hook to intercept keystrokes	1
Contains embedded VBA macros with keywords that indicate auto-execute behavior	1
Contains embedded string that indicates auto-execute behavior	0
Opened the service control manager	1
Opened the service control manager	0
Requested access to a system service	1
Creates new processes	1
Drops executable files	0
Found potential IP address in binary/memory	1
Uses a User Agent typical for browsers, although no browser was ever launched	1
Reads the registry for installed applications	1
Contacts domains	0
Contacts server	1
Contains embedded VBA macros	0
Creates a writable file in a temporary directory	1
Creates mutants	0
Loads rich edit control libraries	1
Loads the .NET runtime environment	0
Process launched with changed environment	1
Scanning for window names	0
Sets a windows hook	1
Spawns new processes	1
Dropped files	0
Opens the MountPointManager	0
Touches files in the Windows directory	0
Hooks API calls	1
Queries sensitive IE security settings	1
Installs hooks/patches the running process	1
Reads information about supported languages	0

O0	O1	O2	
0	0	0	Adware
0	0	1	Spyware
0	1	0	Worm
0	1	1	Trojan
1	0	0	Rootkit
1	0	1	Backdoors
1	1	0	Keyloggers
1	1	1	Rogue
0	0	0	Ransomware
0	0	1	Hijacker

THANK YOU