KISA Korea Internet & Security Agency

Incident Response Using Machine Learning

KISC KrCERT/CC KOREA INTERNET SECURITY CENTER

Minsung(Chris) Jung
Machine Learning Engineer / Data Scientist
KISA (KrCERT/CC)
jmstar85@kisa.or.kr

Agenda

1 What are AI / ML / DL?

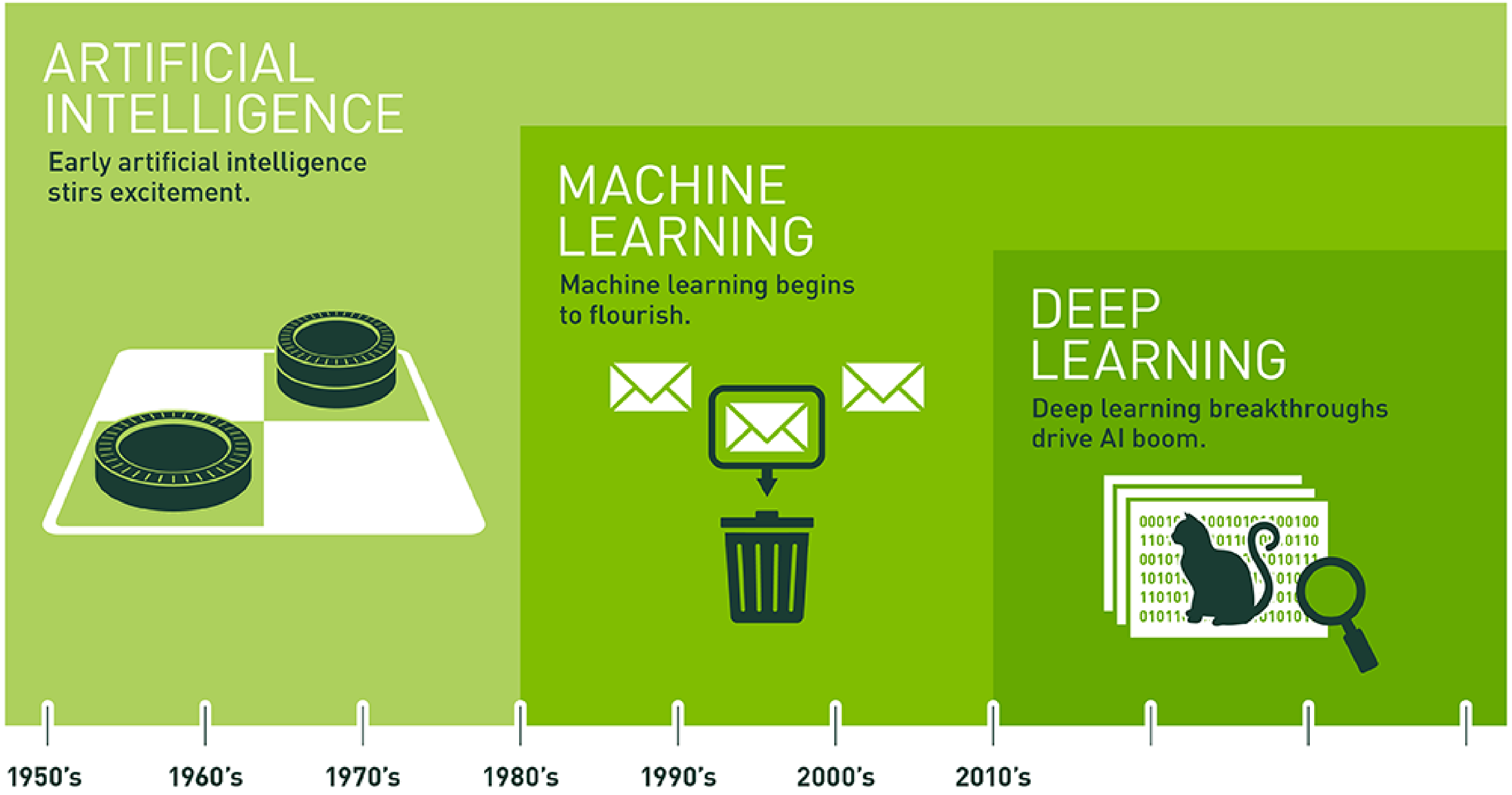
2 How is AI/ML Used in Cyber Security

3 Web Defacement Demo

1

What are AI / ML / DL?

1 What are AI / ML / DL?



ARTIFICIAL INTELLIGENCE

Early artificial intelligence stirs excitement.

MACHINE LEARNING

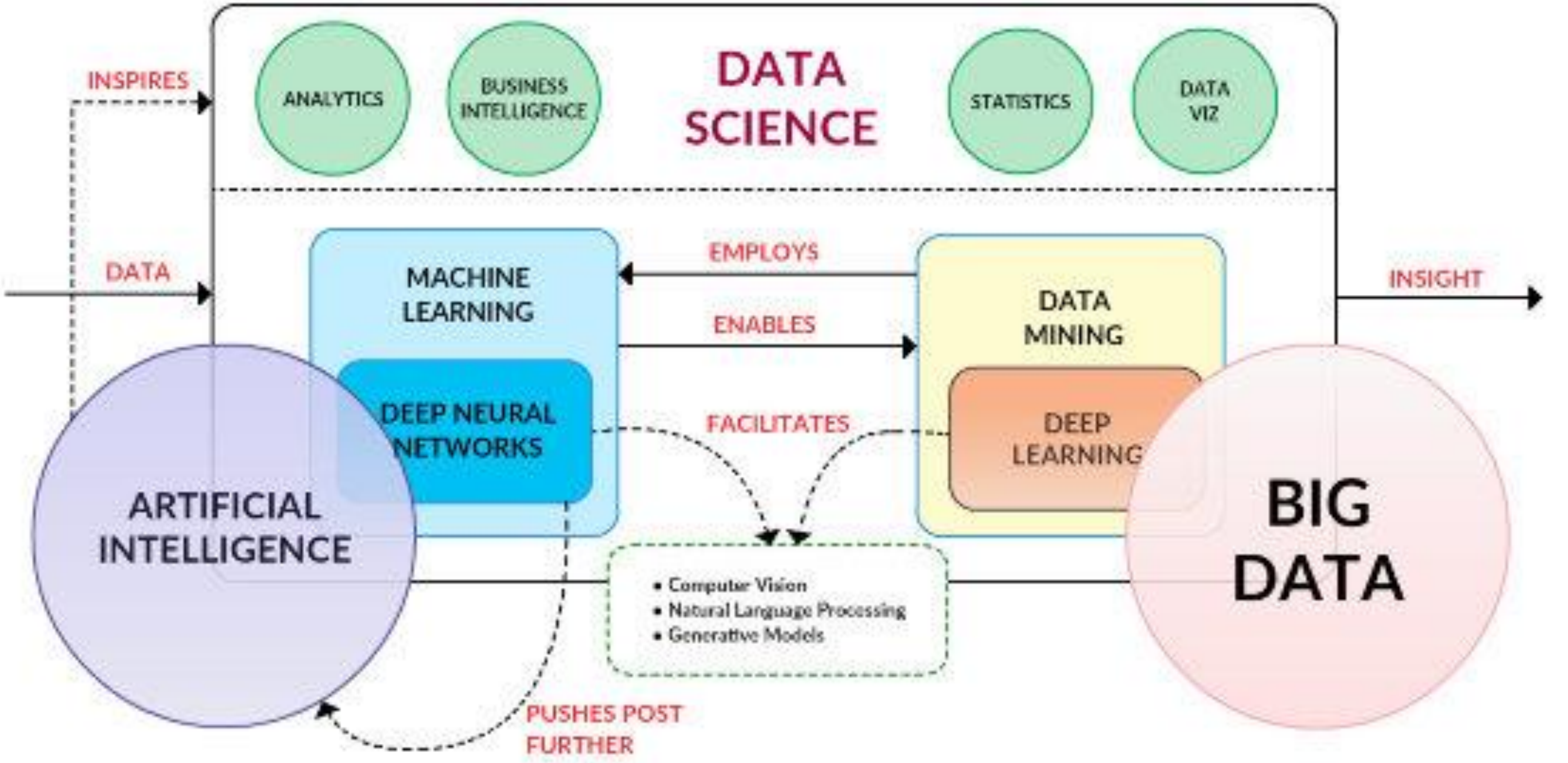
Machine learning begins to flourish.

DEEP LEARNING

Deep learning breakthroughs drive AI boom.

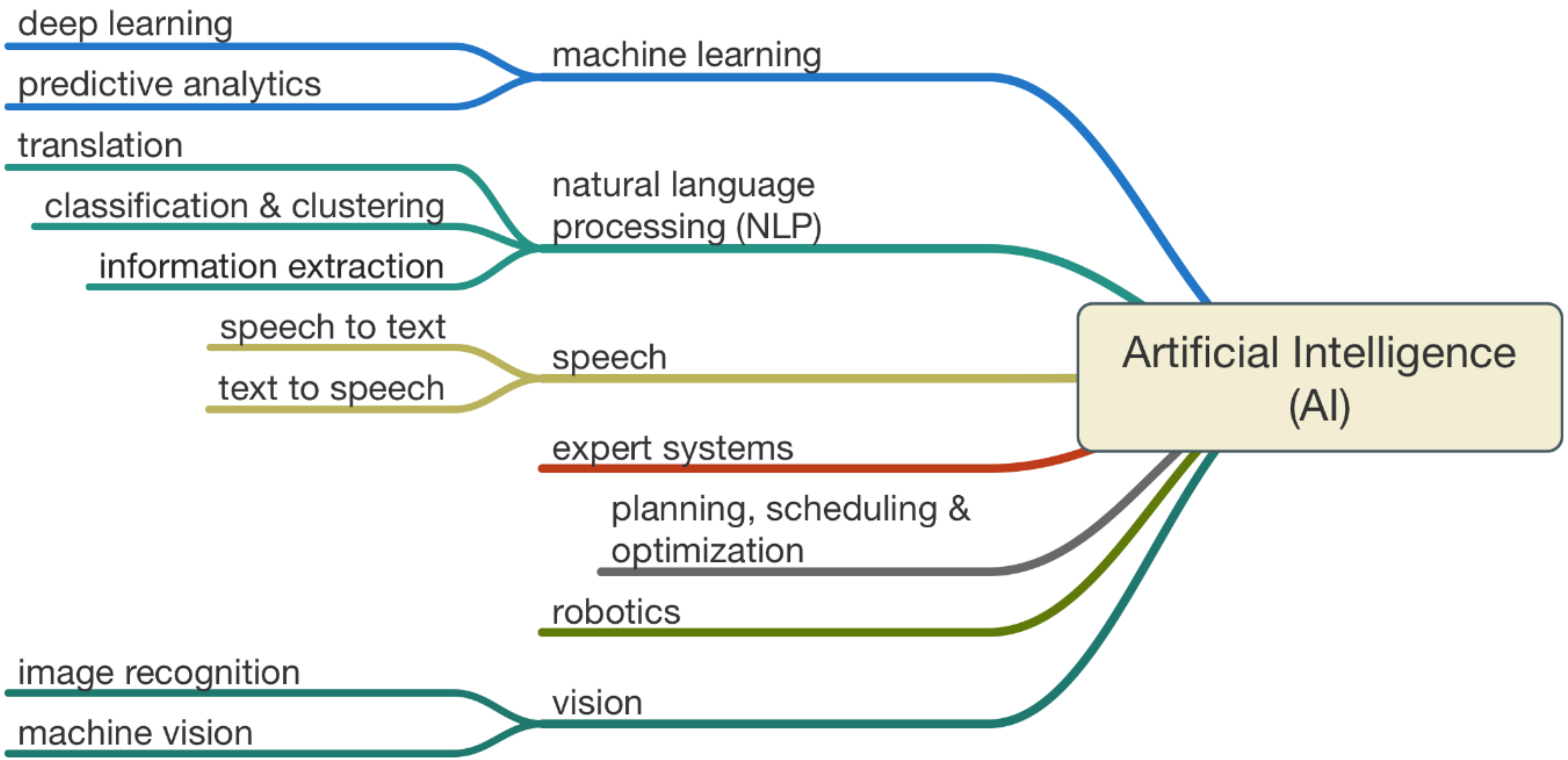
Since an early flush of optimism in the 1950s, smaller subsets of artificial intelligence – first machine learning, then deep learning, a subset of machine learning – have created ever larger disruptions.

What are AI / ML / DL?



1

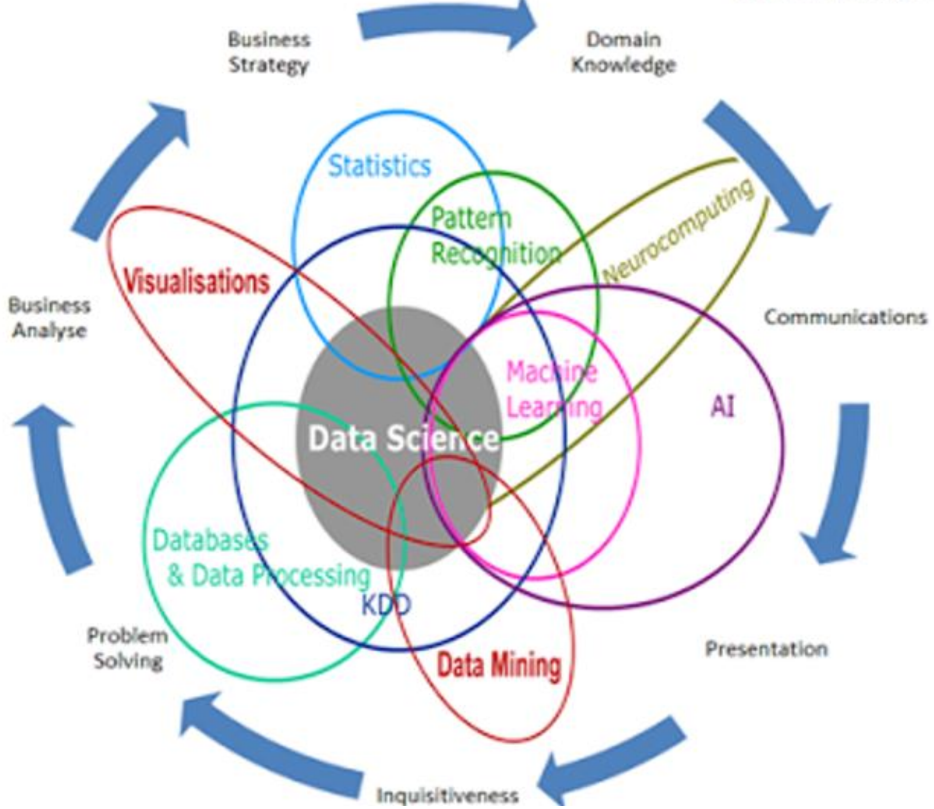
What are AI / ML / DL?



1 What are AI / ML / DL?

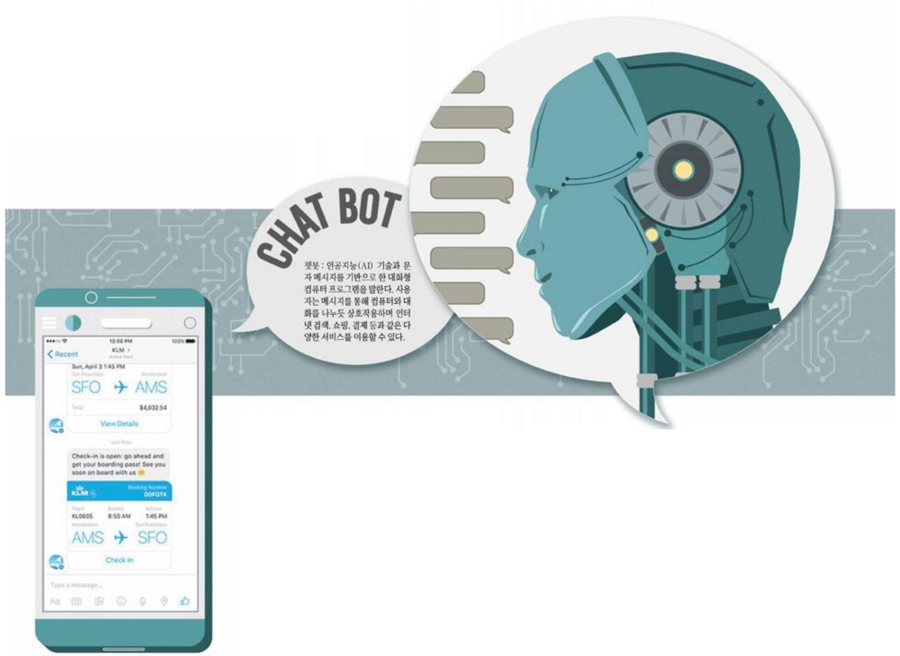
Data Science Is Multidisciplinary

By Brendan Tierney, 2012



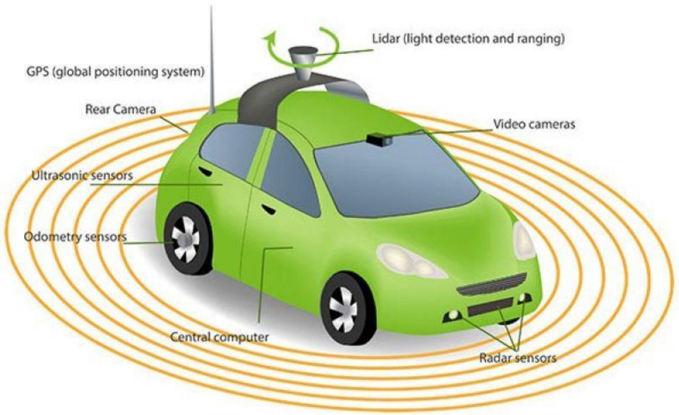
1 ML Examples

- Communicate and Interact with Human



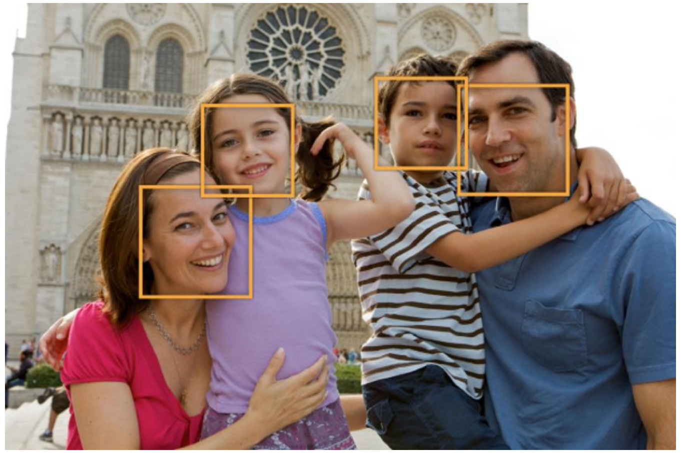
챗봇 : 인공지능(AI) 기술과 문자 메시지를 기반으로 한 대화형 컴퓨터 프로그램을 말한다. 사용자는 메시지를 통해 컴퓨터와 대화를 나누듯 상호작용하며 인터넷 검색, 쇼핑, 결제 등과 같은 다양한 서비스를 이용할 수 있다.

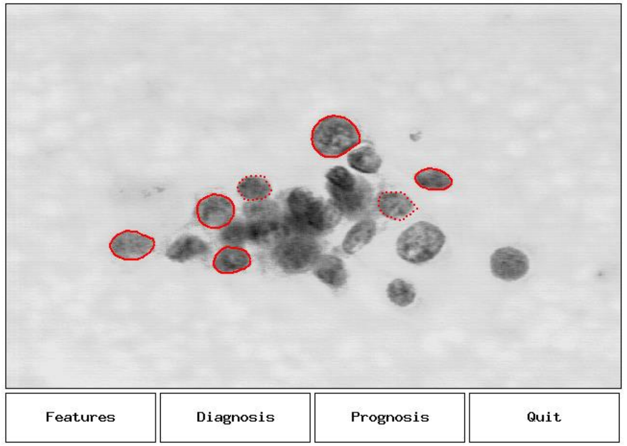
Check-in is open: go ahead and get your boarding pass! See you soon on board with us 😊

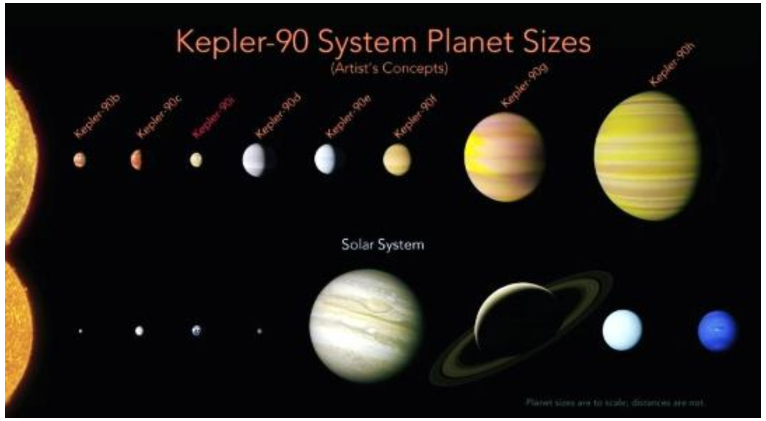


ML Examples

- Analyze factors and classify

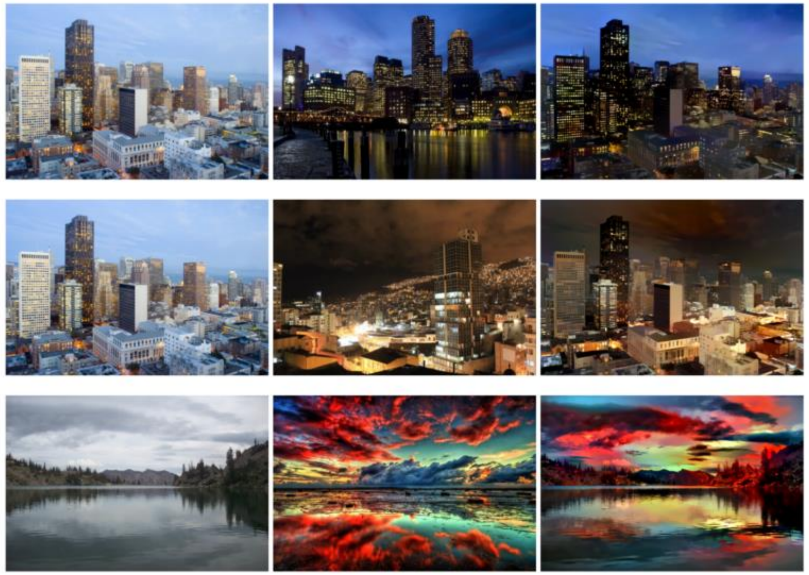


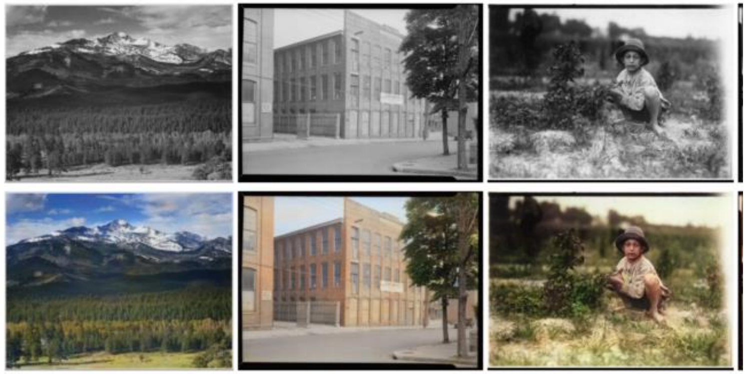




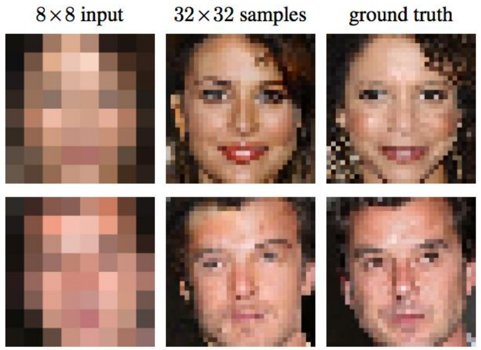
ML Examples

- Possible to do by AI



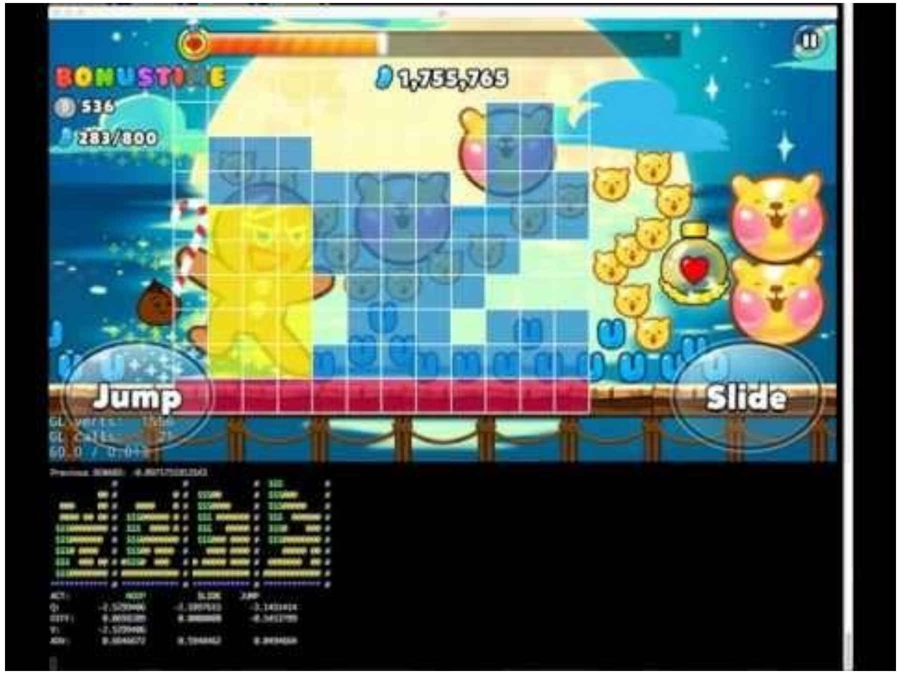


Colorado National Park, 1941 Textile Mill, June 1937 Berry Field, June 1909



ML Examples

- Possible to do by AI

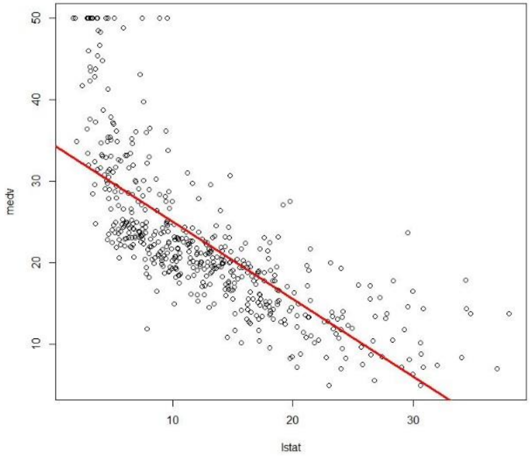


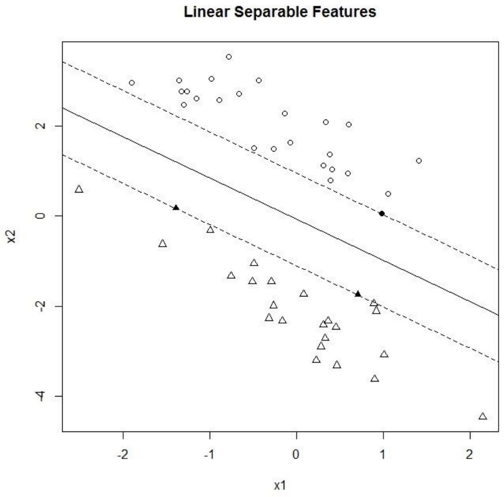
2 How is AI/ML Used in Cyber Security

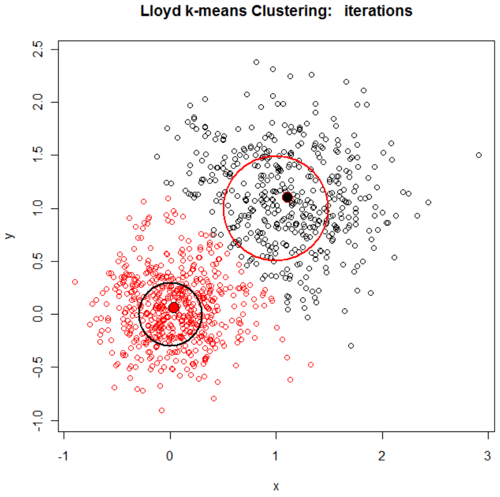
2

How is AI/ML Used in Cyber Security

- **ML Type**
  - Supervised Learning : Yield function by labeled training data (Regression / Classification)
  - Unsupervised Learning : Yield function by unlabeled training data (Clustering)
  - Reinforcement Learning : Learn based on reward



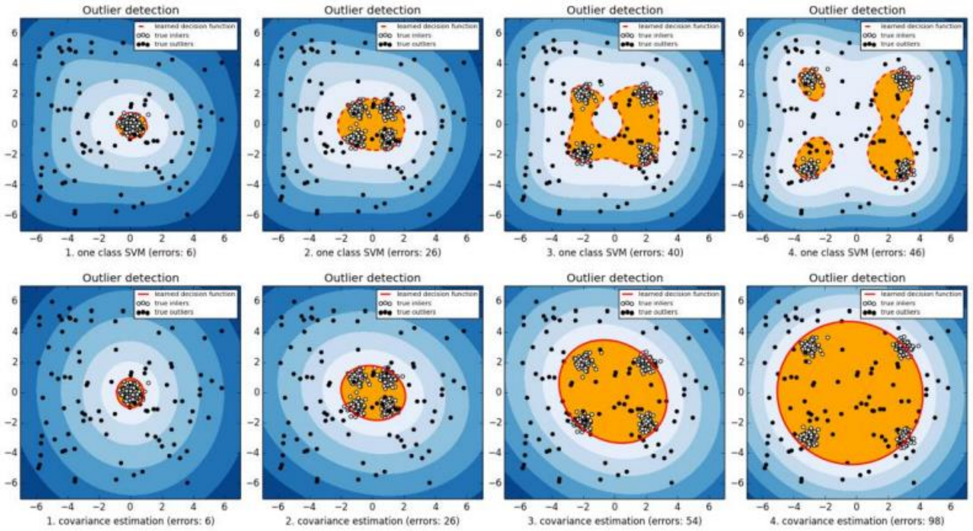




2 How is AI/ML Used in Cyber Security

❖ Anomaly Detection

- ML (using outlier method) is used for anomaly detection based on network traffic models
- Analyze how ‘normal’ labels are distributed and Detect when new data is outlies from the normal sets
- It requires enough amount of data and original signature detection methods



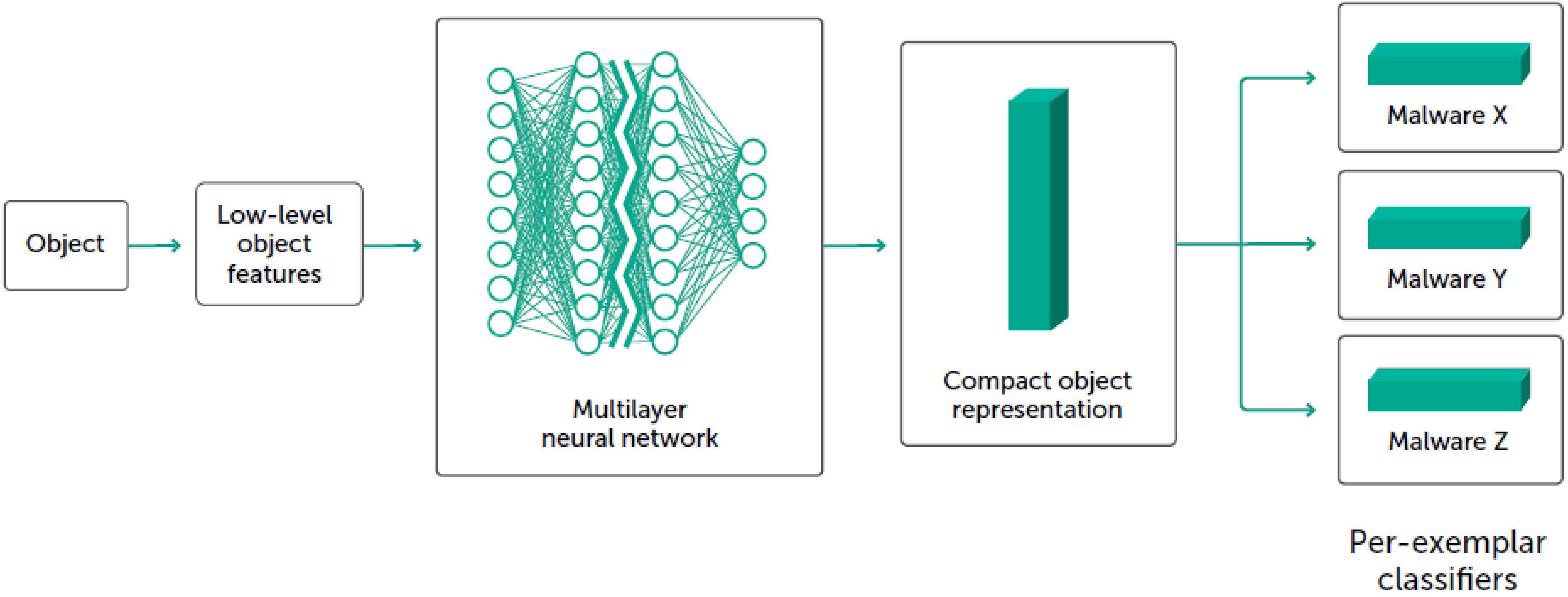
1. one class SVM (errors: 6)
2. one class SVM (errors: 26)
3. one class SVM (errors: 40)
4. one class SVM (errors: 46)
1. covariance estimation (errors: 6)
2. covariance estimation (errors: 26)
3. covariance estimation (errors: 54)
4. covariance estimation (errors: 98)

http://www.hongyusu.com/programming/2015/10/10/novelty-detection/

2

How is AI/ML Used in Cyber Security

- ❖ **Malware Classification**

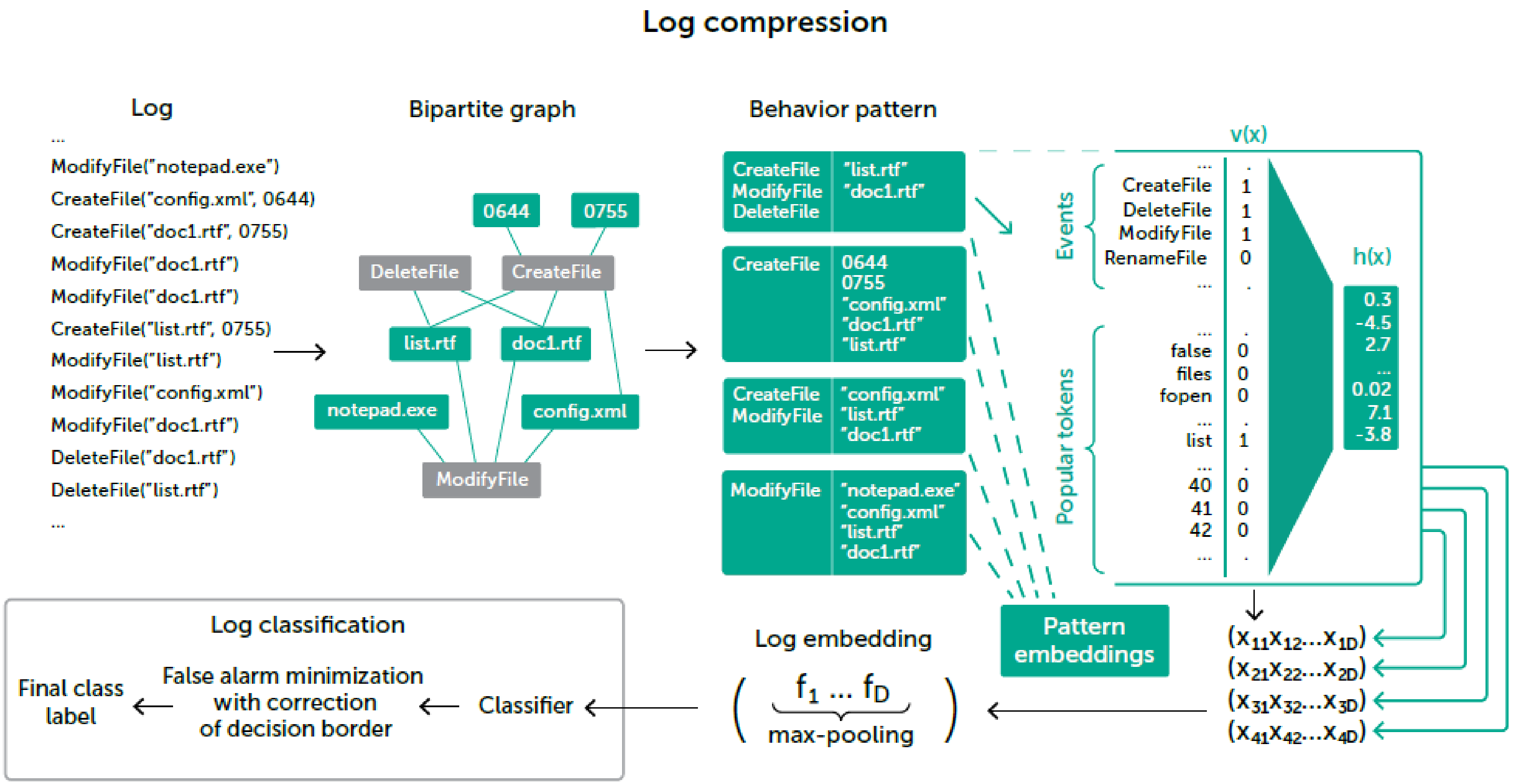

Object
Low-level object features
Multilayer neural network
Compact object representation
Malware X
Malware Y
Malware Z
Per-exemplar classifiers

Machine Learning: exemplar network

2

How is AI/ML Used in Cyber Security

❖ Malware Classification



Log compression

Log

```
...
ModifyFile("notepad.exe")
CreateFile("config.xml", 0644)
CreateFile("doc1.rtf", 0755)
ModifyFile("doc1.rtf")
ModifyFile("doc1.rtf")
CreateFile("list.rtf", 0755)
ModifyFile("list.rtf")
ModifyFile("config.xml")
ModifyFile("doc1.rtf")
DeleteFile("doc1.rtf")
DeleteFile("list.rtf")
...
```

Bipartite graph

Behavior pattern

CreateFile ModifyFile DeleteFile	"list.rtf" "doc1.rtf"
CreateFile	0644 0755 "config.xml" "doc1.rtf" "list.rtf"
CreateFile ModifyFile	"config.xml" "list.rtf" "doc1.rtf"
ModifyFile	"notepad.exe" "config.xml" "list.rtf" "doc1.rtf"

v(x)

Events	...	.
	CreateFile	1
	DeleteFile	1
	ModifyFile	1
	RenameFile	0
	...	.
Popular tokens	...	.
	false	0
	files	0
	fopen	0
	...	.
	list	1
	...	.
	40	0
	41	0
	42	0
	...	.

h(x)

0.3
-4.5
2.7
...
0.02
7.1
-3.8

Pattern embeddings

$(x_{11}x_{12}...x_{1D})$
$(x_{21}x_{22}...x_{2D})$
$(x_{31}x_{32}...x_{3D})$
$(x_{41}x_{42}...x_{4D})$

Log embedding

$$\left(\underbrace{f_1 \ldots f_D}_{\text{max-pooling}} \right)$$

Log classification

Final class label ← False alarm minimization with correction of decision border ← Classifier ←

Machine Learning: behavior model pipeline

3 Web Defacement Demo

3 Web Defacement Demo

TEXT

No	변수	특징값
1	X1	Hacked by
2	X2	Owned by
3	X3	Deface

IMAGE

H1

H2

H3

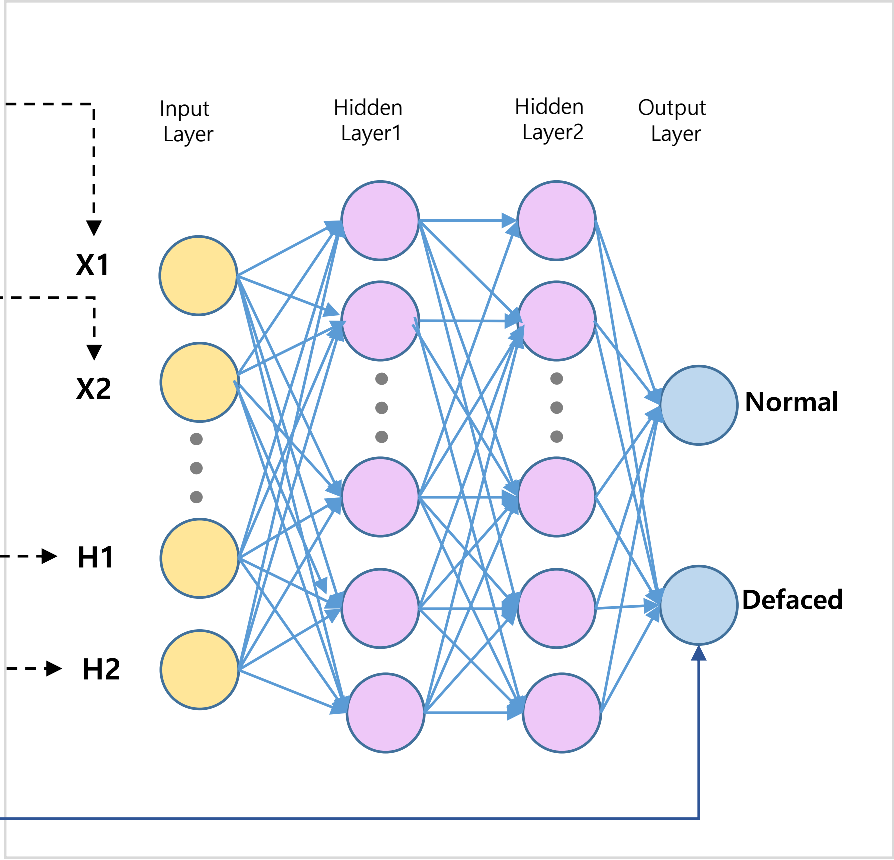
H4

Data sets

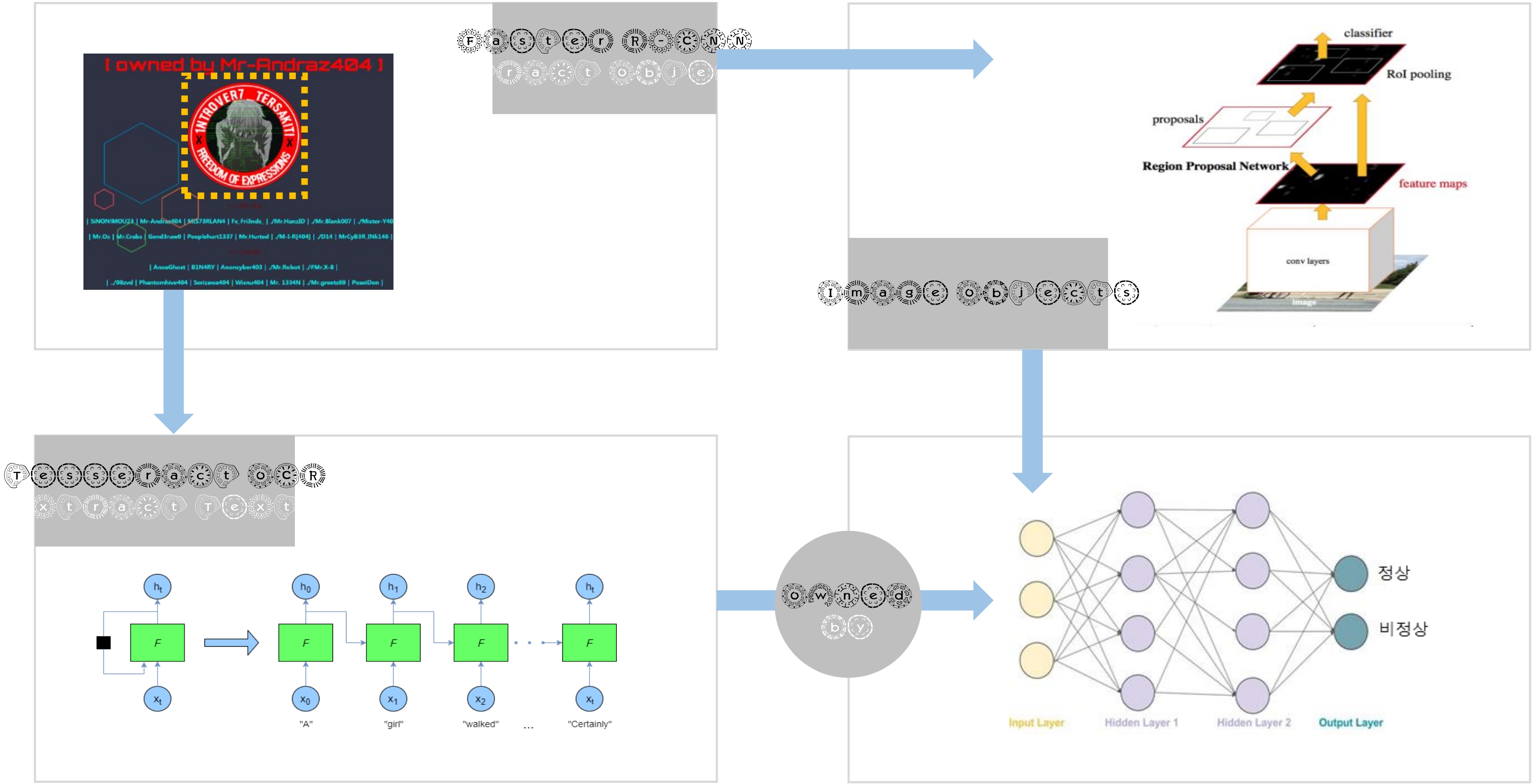
Image/ Variable	x1	x2	…	H1	H2	Web Defaced
0	1	0	0	0	0	1
0	0	1	0	0	0	1
	0	0	0	1	0	1
	0	0	0	0	1	1

3 Web Defacement Demo

Image/ Variable	x1	x2	...	H1	H2	Web Defaced
0	1	0	0	0	0	1
0	0	1	0	0	0	1
	0	0	0	1	0	1
	0	0	0	0	1	1



3 Web Defacement Demo


[owned by Mr-Andraz404]
1NTROVER7 TERSAKITI
FREEDOM OF EXPRESSIONS
| SiNONIMOU23 | Mr-Andraz404 | MIS73RLAN4 | Fx_Fri3nds_ | ./Mr.HanzID | ./Mr.Blank007 | ./Mister-Y40
Mr.Oz	Mr.Crabs	Gend3ruw0	Peoplehurt1337	Mr.Hurted	./M-I-R[404]	./D14	MrCyB3R_INk146
AnoaGhost	B1N4RY	Anoncyber403	./Mr.Robot	./#Mr.X-8
../08zvd	Phantomhive404	Serizawa404	Wisnu404	Mr. 1334N	./Mr.greetz69	PoseiDon
Faster R-CNN
ract obje
classifier
RoI pooling
proposals
Region Proposal Network
feature maps
conv layers
image
Image Objects
Tesseract OCR
xtract Text
h_t
F
x_t
h_0
h_1
h_2
h_t
x_0
x_1
x_2
x_t
"A"
"girl"
"walked"
...
"Certainly"
owned by
정상
비정상
Input Layer
Hidden Layer 1
Hidden Layer 2
Output Layer

Thank you

Minsung(Chris) Jung

Machine Learning Engineer / Data Scientist

+82-10-2680-9672

jmstar85@kisa.or.kr