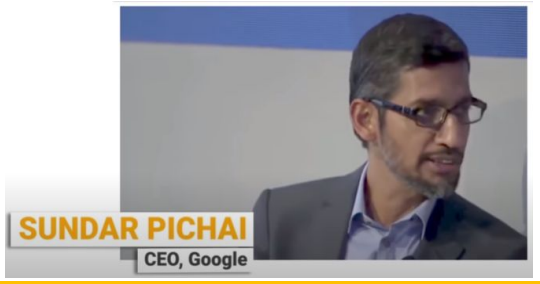
Machine Learning in Social Engineering

By
Abdullah A. Nahi

Contents

I . Introduction to ML & SE

Social engineering attacks are frequent, well-known and easy to apply attacks in the cyber domain. Historical evidence of such attacks has shown that most malicious attempts against both physical and virtual IT systems were based or been initiated using social engineering methods.



AI is the main tool behind new-age innovation and discoveries like driverless cars or disease detecting algorithm

Generalized AI is worth thinking about because it stretches our imaginations, and it gets us to think about our core values and issues of choice

Artificial Intelligence will be ‘vastly smarter’ than any human and would overtake us by 2025.

We are now solving problems with machine learning and AI that were…in the realm of science fiction for the last several decades

Artificial Intelligence and Machine Learning

Artificial Intelligence

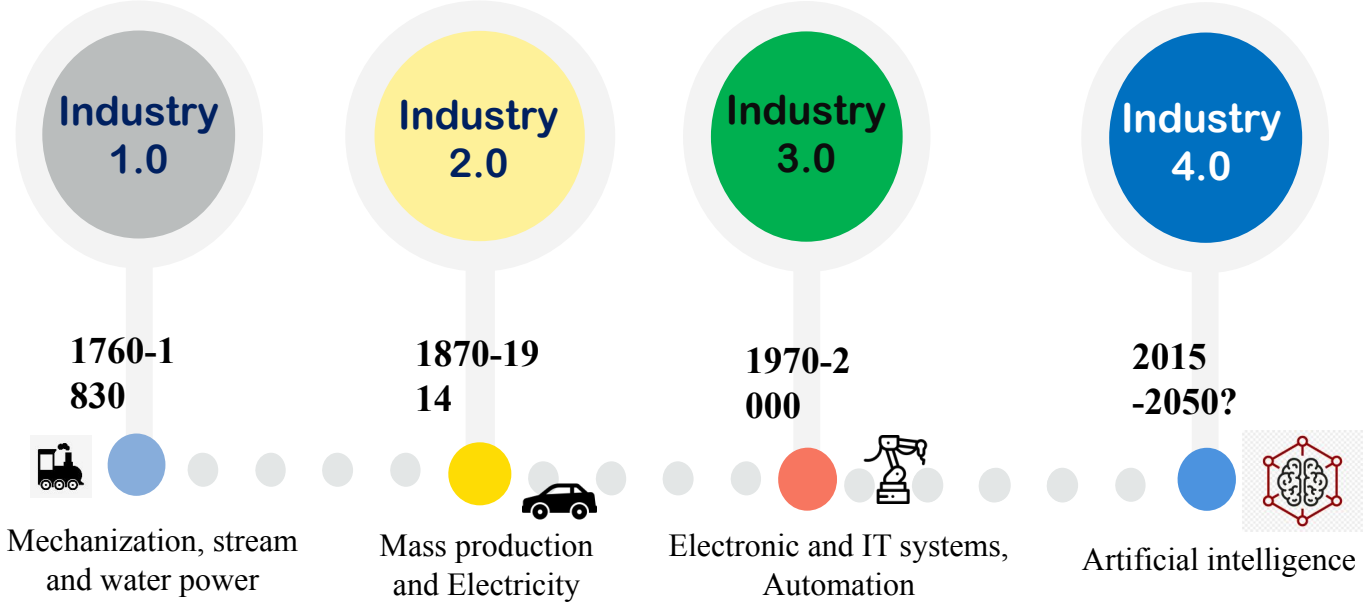
AI is trained final output machine which mimic like human brain
Ex: Amazon Alexa

Machine Learning

ML is a subset of AI. It is a technique to achieve AI. Ex: Spam Detection

Artificial Intelligence and Machine Learning in Industry 4.0

Breakdowns of industrial development and the great changes in related categories



Applications of AI & ML

1. Automated Customer Support

- Online shopping experience has been greatly enhanced by chatbots because of the following reasons:
  - They increase user retention by sending reminders and notifications
  - They offer instant answers compared to human assistants, thus reducing response time
  - Chatbots provide upselling opportunities through personalized approach

2. Personalized Shopping Experience

- Implementation of artificial intelligence makes it possible for online stores to use the smallest piece of data about every followed link or hover to personalize your experience on a deeper level.

- This personalization results into timely alerts, messages, visuals that should be particularly interesting to you, and dynamic content that modifies according to users' demand and supply.

3. Healthcare

- AI-enabled workflow assistants are aiding doctors free up their schedules, reducing time and cost by streamlining processes and opening up new avenues for the industry.

- In addition, AI-powered technology helps pathologists in analyzing tissue samples and thus, in turn, making more accurate diagnosis.

4. Finance

- Automated advisors powered by AI, are capable of predicting the best portfolio or stock based on preferences by scanning the market data.

- Actionable reports based on relevant financial data is also being generated by scanning millions of key data points, thus saving analysts numerous hours of work.

5. Smart Cars and Drones

- With autonomous vehicles running on the roads and autonomous drones delivering the shipments, a significant amount of transportation and service related issues can be resolved faster and more effectively.

6. Travel and Navigation

- With **AI**-enabled mapping, it scans road information and utilizes algorithms to identify the optimal route to take, be it in a bike, car, bus, train, or on foot.

7. Social media

- Face book uses advanced machine learning to do everything from serving content to you and to recognize your face in photos to target users with advertising.
- Instagram (owned by Facebook) uses AI to identify visuals.
- LinkedIn uses AI to offer job recommendations, suggest people you might like to connect with, and serving you specific posts in your feed.

8. Smart Home Devices

- The connected devices of smart homes provide the data and the AI learns from that data to perform certain tasks without human intervention.

9. Creative Arts

- **AI**-powered technologies can help musicians create new themes.

10. Security and Surveillance

- AI is making possible for humans to constantly monitor multiple channels with feeds coming in from a huge number of cameras at the same time.

Avenues

- Hospital and Medicine
- Game Playing
- Speech Recognition
- Understanding Natural Language
- Computer Vision
- Cyber Security
- Face Recognition
- Transport
- Marketing & Advertising

Social Engineering Attacks

As the U.S. National Security Commission on Artificial Intelligence's 2019 interim report notes, a very small percentage of current AI research goes toward defending AI systems against adversarial efforts. Some systems already used in production could be vulnerable to attack. For example, by placing a few small stickers on the ground researchers showed that they could cause a self-driving car to move into the opposite lane of traffic. Other studies have shown that making imperceptible changes to an image can trick a medical analysis system into classifying a benign mole as malignant, and that pieces of tape can deceive a computer vision system into wrongly classifying a stop sign as a speed limit sign.

World’s biggest companies heavily relying on AI & ML


amazon web services
IBM
phrasee
lesforce
Alibaba Cloud
Google Cloud Platform
sift
Microsoft Azure
ANDURIL
people.ai
nauto
certis
Applied Cloud
SIEMENS
DATAVISOR
AUTOMATION ANYWHERE
RPV
AEYE
AlphaSense
VERKADA
SenSat
Suki
freenome
intel
NVIDIA
Orbital Insight
IRIS.AI


zebra
MEDICAL.VISION


clarifai


pymetrics


tamr


flatiron


defined
crowd


Tencent 腾讯


xnor.ai


next IT


ViSENZE
Simplifying the Visual Web


pony.ai


商汤
sensetime


bigpanda


bossanova

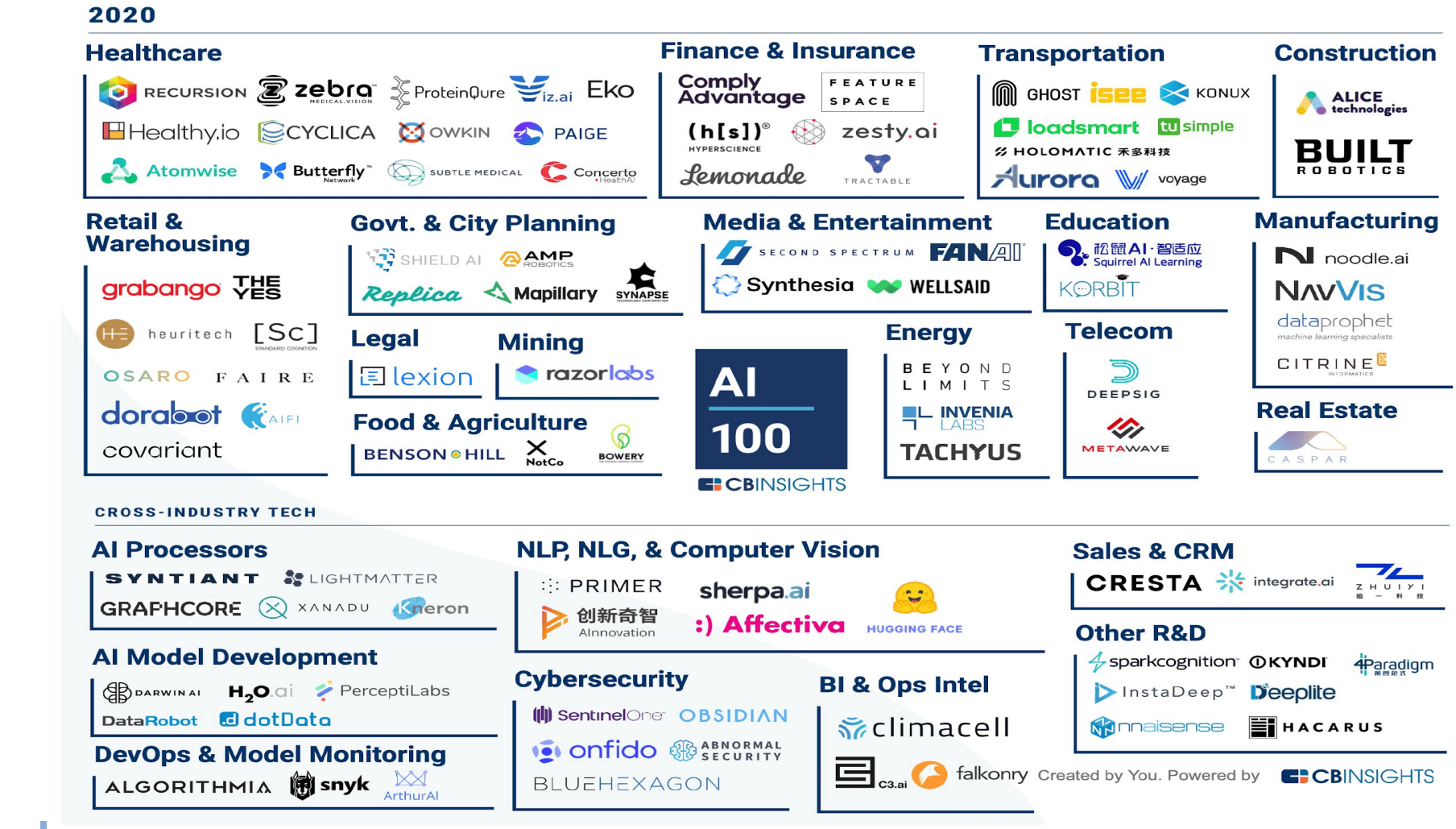

DEEP 6 AI


ELEMENT AI


C3.ai

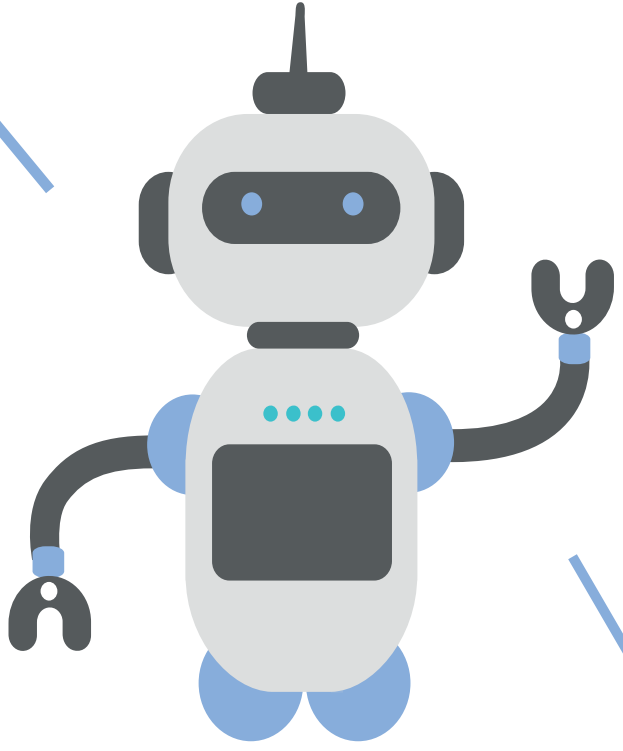

directly


Enterprise AI Companies
Presented by
TOPBOTS
Business Intelligence
Productivity
Customer Management
HR & Talent
B2B Sales & Marketing
Consumer Marketing
Finance & Operations
Digital Commerce
Data Science
Engineering
Security & Risk
Industrials & Manufacturing
TRADESHIFT
LOGILITY
VECTRA
skuchain
PENSIAMO
ZIMPERIUM.
narvar
DRAWBRIDGE NETWORKS
PREDIX
CYLANCE
fusionops
kinaxis
SIGNALSENSE
graphistry
DEMISTO
deepvu
deepinstinct
sift science
ARIMO
SentinelOne
DARKTRACE
Anodot
sparkcognition
signifai
BONSAI AI
fuzzyai
kite
Cycorp
logz.io
DIFFBOT
rainforest
bigml
context relevant
data iku
DataRobot
CrowdFlower
rapidminer
DOMINO
SPARKBEYOND
DATALOGUE
deepsense.io
SIGOPT
ŷhat
msg.ai
bloomreach
wayblazer
sentient
Artificia
optoro
LAYER 6
SiteZeus
InfiniteAnalytics
MONA
SNAPSHOPS
sas
TRIFACTA
tamr
yseop
SISENSE
Paxata
MAANA
enigma
DATASIFT
NarrativeScience
AYASDI
import.io
Alation
sapho
CognitiveScale
WorkFusion
captricity
AppZen
(h [s])
xono
FreeBusy
talla
Julie Desk
SKIPFLAG
DigitalGenius
Zoom.ai
nextos
CLARABRIDGE
Brainasoft
pogo
inbenta
COGNICOR
Kasisto
zendesk
clara
IPSOFT
interactions
LUMINOSO
Preact
narvar
ACTIONIQ
LIVEPERSON
Wise.io
ELOQUENT
GIGSTER
Scout
textio
Unitive
SpringRole
HireVue
entelo
hiQ
Wade&Wendy
collectiveIQ
AVISO
6sense
conversica
fuse|machines
Lattice
clari
brightfunnel
RADIUS
Appier
gumgum
insidesales.com
MINTIGO
LEXALYTICS
Albert
LiftIgniter
AIRPR
einstein
[PERSADO]
RESCI
Zensight
NETBASE™
INVOCA
TACT


2020
Healthcare
RECURSION
zebra MEDICAL VISION
ProteinQure
iz.ai
Eko
Healthy.io
CYCLICA
OWKIN
PAIGE
Atomwise
Butterfly Network
SUBTLE MEDICAL
Concerto HealthAI
Finance & Insurance
Comply Advantage
FEATURE SPACE
(h[s])
HYPERSCIENCE
zesty.ai
Lemonade
TRACTABLE
Transportation
GHOST
isee
KONUX
loadsmart
tusimple
HOLOMATIC 禾多科技
Aurora
voyage
Construction
ALICE technologies
BUILT ROBOTICS
Retail & Warehousing
grabango
THE YES
heuritech
[Sc]
STANDARD COGNITION
OSARO
FAIRE
dorabot
AIFI
covariant
Govt. & City Planning
SHIELD AI
AMP ROBOTICS
Replica
Mapillary
SYNAPSE
Legal
lexion
Mining
razorlabs
Food & Agriculture
BENSON HILL
NotCo
BOWERY
Media & Entertainment
SECOND SPECTRUM
FANAI
Synthesia
WELLSAID
Education
松鼠AI·智适应
Squirrel AI Learning
KORBIT
Manufacturing
noodle.ai
NavVis
dataprophet
machine learning specialists
CITRINE INFORMATICS
Real Estate
CASPAR
AI 100
CBINSIGHTS
Energy
BEYOND LIMITS
INVENIA LABS
TACHYUS
Telecom
DEEPSIG
METAWAVE
CROSS-INDUSTRY TECH
AI Processors
SYNTIANT
LIGHTMATTER
GRAPHCORE
XANADU
Kneron
AI Model Development
DARWIN AI
H2O.ai
PerceptiLabs
DataRobot
dotData
DevOps & Model Monitoring
ALGORITHMIA
snyk
ArthurAI
NLP, NLG, & Computer Vision
PRIMER
sherpa.ai
創新奇智
AInnovation
Affectiva
HUGGING FACE
Cybersecurity
SentinelOne
OBSIDIAN
onfido
ABNORMAL SECURITY
BLUEHEXAGON
BI & Ops Intel
climacell
C3.ai
falkonry
Sales & CRM
CRESTA
integrate.ai
ZHUIYI
Other R&D
sparkcognition
KYNDI
4Paradigm
InstaDeep
Deeplite
nnaisense
HACARUS
Created by You. Powered by
CBINSIGHTS

III. AI & ML to drive growth of Start ups

- Startups ecosystem, has been nourished with the advent of technology, and has given rise to more evolved business processes.
- These days Logistics, accounts, marketing and team performance & HR have all been supported by AI technology.



- With the rising technologies like AI, IoT and ML, its interesting to watch the changing face of Indian SMEs and startups.

V. Conclusions

- As an Artificial Intelligence aspirant, you have ample of job opportunities in this field.
- Artificial intelligence will transform the global economy, and AI jobs are in high demand.
- According to International Data Corporation (IDC), the number of AI jobs is expected to globally grow 16 percent this year.
- AI careers are future-proof, meaning they are likely to survive well into the future.
- Getting an education in AI is challenging and requires persistence and personal initiative.

THANK YOU