AI AND CYBERSECURITY

GROUP 10

ALLOUI MOHAMED, BAUQUIN NIELS, DOUZI YOUSSEF, KALLEL MOHAMED ALI | COMPUTER SCIENCE MASTER 2024/2025

SUPERVIZED BY : ***SCHATZ THOMAS***

amU Aix Marseille Université

Introduction

Cybersecurity: a key issue in the digital age:

- Protect systems, networks and data against cyberthreats.

Main objectives :

- **Confidentiality**: guarantee the security of information.
- **Integrity**: prevent unauthorized alteration of data.
- **Availability**: ensure continuous access to systems and services

Common threats :

- Malware, ransomware and phishing attacks.
- Exploitation of system vulnerabilities.

Current challenges :

- Increasing complexity of attacks
- Increasing need for innovative solutions such as **NLP** and **Federated Learning**.

Cybersecurity Market

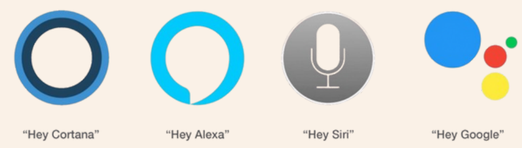
Période d'étude	2019 - 2029
Taille du Marché (2024)	USD 234.01 Billion
Taille du Marché (2029)	USD 424.14 Billion
CAGR (2024 - 2029)	11.44 %
Marché à la Croissance la Plus Rapide	Asie-Pacifique
Plus Grand Marché	Amérique du Nord
Concentration du Marché	Faible
Acteurs majeurs	proofpoint. NortonLifeLock IBM Microsoft McAfee

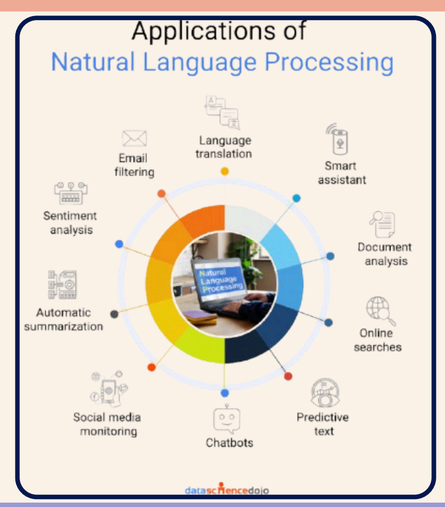
Source : Mordor Intelligence

Natural langage processing

What is it and why it is used:

Natural language processing (NLP) is the ability of a computer program to understand human language as it's spoken and written -- referred to as natural language. It's a component of artificial intelligence (AI).





How NLP works

Data collection and cleansing :

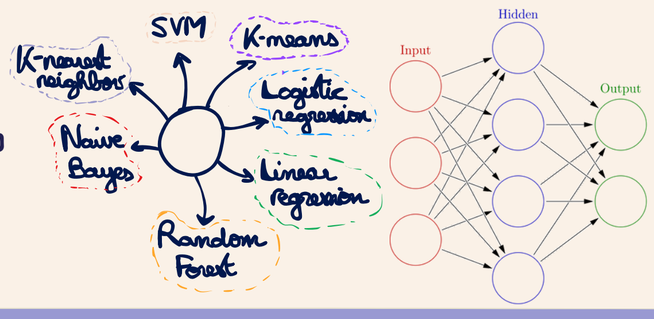
- Tokenization: Division of text into basic units (words, syllable groups). Example: [bonjour comment ça va ?] becomes ["Bonjour" , "comment" , "ça" , "va" , "?"].
- Elimination of Stop-words : Elimination of common but non-affirmative words (LE , DE , ET , LA)
- Stemming and Lemming :
  - Stemmatization: Reduction of a word to its root, which may be grammatically false, the and made by heuristic algorithms by removing prefixes and suffixes
  - Lemmatization: A more sophisticated method that reduces a word to its lemma, its canonical form, based on linguistic rules.

Words representation: Transformation of words into a form that machine learning algorithms can understand: numerical vectors

- Bags of Word: each document is represented by a vector of the frequency with which words appear in the document
- TF-IDF: An enhancement to BoW that weights words according to their importance by applying the following formula:
  - TF-IDF = TF x log(N/DF) where DF = number of documents containing the word, N = number of documents TF= Frequency of the word in the document.

Processing with AI models:

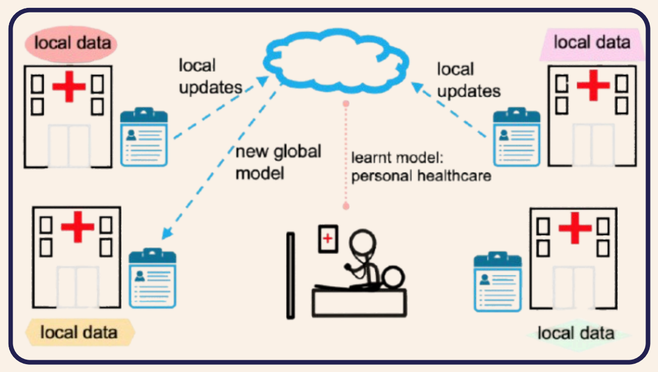
- Classical approaches :
  - Regressions (Linear, Logistic)
  - Probabilistic models (Naive Bayes)
  - SVM
- Modern approaches :
  - Transformers (Bert, GPT)
  - RNN (Recurrent Neural Networks)



Federated Learning

Definition:

Federated Learning is a machine learning technique where **data** remains on **local** devices, and only **models** or parameter **updates** are **shared**

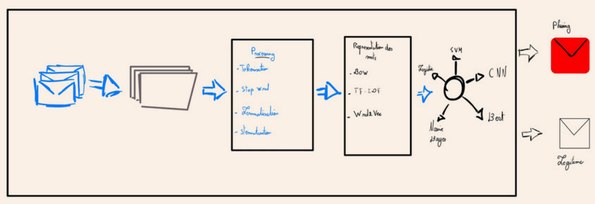


Cybersecurity advantages:

- Privacy **protection** by minimizing the transfer of sensitive data.
- The system is more **resilient** in the face of **DDoS** or **ransomware** attacks, which often target centralized databases.
- Connected devices (such as smartphones, IoTs) can **detect malicious patterns locally** and help improve a global model without directly sharing sensitive logs. This enables emerging threats to be detected **quickly**, while maintaining a **high level of security**.

Model updates are aggregated and encrypted, limiting the possibilities for a malicious actor to interfere or access data.

Application to cyber security: Pishing detection



AI relies on **data**. Therefore, using AI to protect ourselves leads us to think about how to **secure** that data.

Security risks

Data poisoning attacks:

- A malicious participant modifies or inserts incorrect, biased or malicious data into his own training set.
- Local models trained with this biased data introduce errors into the global model after aggregation.

Model poisoning attacks :

- A compromised participant locally trains a model with malicious objectives.
- During the aggregation stage, it sends modified updates to the server.
- As the server integrates these updates, it gradually adopts undesirable behaviors.

Conclusion

Artificial intelligence transforms cybersecurity:

- Advanced threat detection.
- Powerful **predictive analysis**.
- **Automated** responses.

Data centralization **challenges**:

- Increased **vulnerability** to cyber-attacks.
- Confidentiality and ethical **issues**.

Federated Learning combines the efficiency of AI and decentralized models:

- **Reducing** the risks associated with data concentration.

Federated Learning: a promising but imperfect alternative :

- Reduces the risks associated with data centralization.

Still vulnerable to specific attacks:

— **Data poisoning** : contamination of learning data.

— **Model poisoning**: alteration of AI models.

Conclusion: an evolving field

- There are still many challenges to the resilience and effectiveness of AI in cybersecurity.
- The need to develop complementary solutions to enhance security.

Bibliography

- Priyanka Mary Mammen. (2021). Federated Learning: Opportunities and Challenges. University of Massachusetts.
- Iqbal H. Sarker. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions.
- Joseph Nnaemeka Chukwunweike , Moshood Yussuf , Oluwatobiloba Okusi. The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions.
- Bibhu Dash, Meraj Farheen Ansari, Pawankumar Sharma and Azad Ali. THREATS AND OPPORTUNITIES WITH AIBASED CYBER SECURITY INTRUSION DETECTION: A REVIEWDept. of Computer and Information Systems, University of the Cumberlands, Williamsburg, KY USA. 1
- JOON-WOO LEE, WOOSUK CHOI, JIEUN EOM. Privacy Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural NetworkDept. of Computer and Information Systems, University of the Cumberlands, Williamsburg, KY USA.
- Phishing Detection Using Natural Language Processing and Machine Learning Apurv Mittal
- Qu'est-ce que le PNL (Traitement du Langage Naturel) ? IBM technology
- The Role of Artificial Intelligence in Cyber-Defence — AI Cybersecurity — Vincent Lenders
- Entretien avec Mr.Nasraoui (ingénieur en cybersécurité)
- Natural Language Processing , Jacob Eisenstein