L'IA ET CYBERSÉCURITÉ

GROUPE 10
ALLOUI MOHAMED, BAUQUIN NIELS, DOUZI YOUSSEF, KALLEL MOHAMED ALI | MASTER INFORMATIQUE 2024/2025
SUPERVISÉ PAR : SCHATZ THOMAS

Aix Marseille Université

Introduction

Cybersécurité : un enjeu clé à l'ère numérique :

- Protège les systèmes, réseaux et données contre les cybermenaces.

Principaux objectifs :

- **Confidentialité** : garantir la sécurité des informations.
- **Intégrité** : prévenir toute altération non autorisée des données.
- **Disponibilité** : assurer un accès continu aux systèmes et services.

Menaces courantes :

- Attaques par malware, ransomware et phishing.
- Exploitation des vulnérabilités des systèmes.

Défis actuels :

- Complexité croissante des attaques.
- Besoin accru de solutions innovantes comme le **NLP** et le **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

Quoi :

Le Natural Language Processing (NLP), ou traitement automatique des langues, est un domaine de l'intelligence artificielle qui se concentre sur l'interaction entre les ordinateurs et le langage humain.

Pourquoi :

Permet aux machines de comprendre, d'analyser, de générer et d'interpréter le langage humain.

Fonctionnement du NLP

Collecte et nettoyage des données :

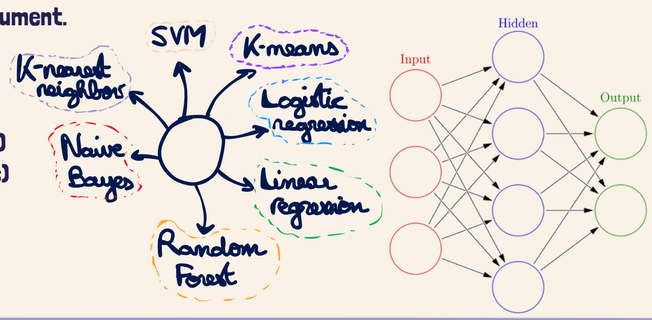
- Tokenisation : Division du texte en unités de base (mots, groupe de syllabes). Exemple : [bonjour comment ça va ?] devient ["Bonjour" , "comment" , "ça" , "va" , "?"]
- Suppression des Stop-words : Élimination des mots courants mais non affirmatifs (LE , DE , ET , LA)
- Stemmatisation et Lemmatisation :
  - Stemmatisation : Réduction d'un mot à sa racine, cette racine peut être fausse grammaticalement, le et faite par des algorithmes heuristiques en supprimant les préfixes et suffixes
  - Lemmatisation : Méthode plus sophistiquée qui ramène un mot à son lemme, sa forme canonique. cette méthode se repose sur des règles linguistiques

Représentations des mots : Transformation des mots en une forme que les algorithmes de machine Learning peuvent comprendre : vecteurs numériques

- Bags of Word : chaque document est représenté par un vecteur de fréquence d'apparition des mots dans le document
- TF-IDF : Une amélioration de BoW qui pondère les mots en fonction de leur importance en appliquant la formule suivante :
  - TF-IDF = TF x log(N/DF) où DF = nombre de document contenant le mots, N = nombre documents TF= Fréquence du mot dans le document.

Traitement avec des modèles d'IA :

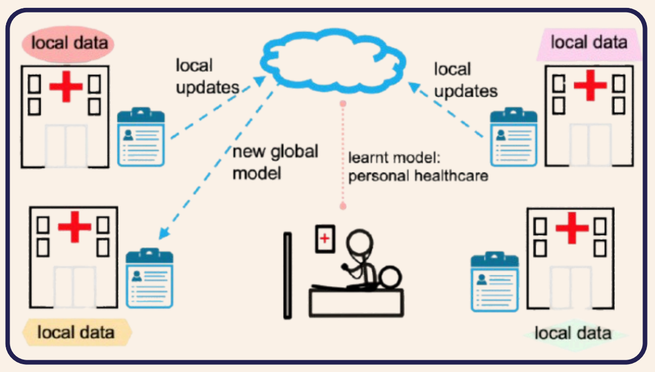
- Approches classiques :
  - Régressions (Linéaire, Logistique)
  - Modèles probabilistes (Naïf Bayes)
  - SVM
- Approches modernes :
  - Transformers (Bert, GPT)
  - RNN (Recurrent neural Networks)



Le Federated Learning

Définition :

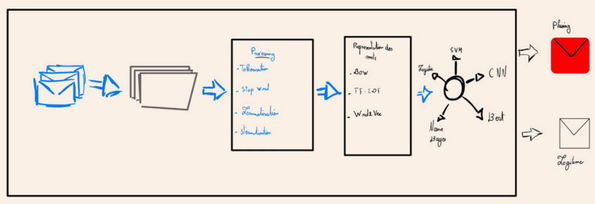
Le Federated Learning (apprentissage fédédré) est une technique d'apprentissage machine où les données restent sur les appareils locaux, et seuls les modèles ou les mises à jour des paramètres sont partagés



Avantages pour la cybersécurité :

- **Protection** de la vie privée en minimisant le transfert de données sensibles.
- Le système est plus **résilient** face aux attaques par déni de service (**DDoS**) ou par **ransomware**, qui ciblent souvent les bases de données centralisées.
- Les appareils connectés (comme les smartphones, les IoT) peuvent **détecter** des **schémas malveillants localement** et contribuer à améliorer un modèle global sans partager directement les logs sensibles. Cela permet de détecter les menaces émergentes **rapidement**, tout en maintenant un **haut niveau** de **sécurité**.
- Les **mises à jour** des modèles sont **agrégées** et **chiffrées**, ce qui limite les possibilités pour un acteur malveillant d'interférer ou d'accéder aux données.

Application à la cyber-sécurité : Pishing détection



L'IA repose sur les **données**. Par conséquent, utiliser l'IA pour se protéger nous amène à réfléchir à la manière de **sécuriser** ces données.

Les risques de securité

Data poisoning attacks :

- Un participant malveillant modifie ou insère des données incorrectes, biaisées ou malveillantes dans son propre ensemble d'entraînement.
- Les modèles locaux formés avec ces données biaisées introduisent des erreurs dans le modèle global après agrégation.

Model poisoning attacks :

- Un participant compromis entraîne localement un modèle avec des objectifs malveillants.
- Lors de l'étape d'agrégation, il envoie des mises à jour modifiées au serveur.
- Le serveur, en intégrant ces mises à jour, adopte progressivement des comportements indésirables.

Conclusion

L'intelligence artificielle transforme la cybersécurité :

- Détection avancée des menaces.
- **Analyse prédictive** performante.
- **Automatisation** des réponses.
- **Défis** liés à la centralisation des données :
- **Vulnérabilité** accrue aux cyberattaques.
- **Problèmes** de confidentialité et enjeux éthiques.

Le Federated Learning combine l'efficacité de l'IA et des modèles décentralisés :

- **Réduction** des **risques** liés à la concentration des données.

Federated Learning : une alternative prometteuse mais imparfaite

- Réduit les risques liés à la centralisation des données.
- Reste vulnérable à des attaques spécifiques :

– **Data poisoning** : contamination des données d'apprentissage.
– **Model poisoning** : altération des modèles d'IA.

Conclusion : un champ encore en évolution

- Les défis en matière de résilience et d'efficacité de l'IA en cybersécurité restent nombreux.
- Nécessité de développer des solutions complémentaires pour renforcer la sécurité.

Sources

- 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