Abdelhak Bouayad

College of Computing
Ben-Guérir, Morocco

email
Webpage

Research Interests

My research interests encompass artificial intelligence, machine learning, and privacy, with a particular focus on the intersection of privacy and machine learning. I develop and apply algorithms and protocols to protect sensitive data in machine learning models, safeguarding against malicious exploitation. My goal is to advance techniques that ensure data privacy while maintaining the efficacy of AI systems.

Education

Mohammed VI Polytechnic University — October 2019 – Present
Ph.D. Computer Science — *Ben-Guérir, Morocco*
- Scientific Director: Ismail Berrada[‡]

Sidi Mohamed Ben Abdellah University — October 2016 – June 2018
M.Sc. Big Data Analytics and Smart Systems. — *Fès, Morocco*
- Thesis: "Lip reading or recognizing what is being said solely depending on the lip movement of the speaker."
- Advisor: Mostafa HARTI

Sidi Mohamed Ben Abdellah University — October 2012 – June 2016
B.A. Mathematics and Computer Science. — *Fès, Morocco*

Research Experience

Research Assistant — October 2019 – Present
College of Computing — *Mohammed VI Polytechnic University*

Publications[†]

Hamza Alami, Ismail Berrada,**Abdelhak Bouayad**, Meryem Janati Idrissi.
NF-NIDS: Normalizing Flows for Network Intrusion Detection Systems. In the 10^{th} International Conference on Wireless Networks and Mobile Communications (**WINCOM**) 2023.
Hamza Alami, Ismail Berrada,**Abdelhak Bouayad**, Meryem Janati Idrissi, Zakaria Yartaoui.
Investigating Domain Adaptation for Network Intrusion Detection. In the 10^{th} International Conference on Wireless Networks and Mobile Communications (**WINCOM**) 2023.

[‡]Professor at college of computing.
[†]Authorship is in **alphabetical** order.

Papers Under Submission

Hamza Alami, Mohammed Akallouch, Ismail Berrada,**Abdelhak Bouayad**.
On the Atout Ticket Learning Problem for Neural Networks and its Application in Securing Federated Learning Exchange
Hamza Alami, Ismail Berrada,**Abdelhak Bouayad**, Meryem Janati Idrissi.
Enhancing ICS Security with Lightweight-Fed-NIDS: Federated Learning and Pruning for Efficient Network Intrusion Detection Systems

Talks

Talk: Sparsification in deep learning: Improving efficiency without sacrificing performance . *Presented at UM6P interdisciplinary workshop 2023.*
Talk :Privacy-Preserving Machine Learning. *Presented at UM6P journée des doctorants 2022.*
Talk: When machine Learning meets cryptography. *Presented at UM6P journée des doctorants 2021.*
Talk: Attacks and defenses in FL. *Presented at UM6P college of computing seminars 2020.*

Projects

Efficient and Accurate Intrusion Detection via Federated Learning: The implementation of a light-weight and fast-learning network intrusion detection machine-learning model for industrial control system that can be trained and deployed on edge devices with limited computing capacity.

Privacy-Preserving Federated Learning with Atout Ticket Learning: Development of a secure federated learning system using Atout Ticket Learning (ATL) to identify and protect sensitive neural network parameters. This system employs the Atout Ticket Protocol (ATP) to ensure data privacy through encryption and minimal parameter alteration, enabling safe data exchanges in federated learning environments.

Distributed K-Nearest Neighbors Algorithm in Java: Developed and implemented a distributed K-Nearest Neighbors (KNN) algorithm using Java, enabling efficient and scalable data classification across multiple nodes

Lip Reading System for Speech Recognition: Developed a system for recognizing speech solely based on the lip movements of the speaker, enabling accurate lip reading.

Kaggle Competitions:
- **Click-Through Rate Prediction**: Predicted whether a mobile ad will be clicked or not.
- **Zillow's Home Value Prediction**: Forecasted home values using various features.
- **Statoil Ship vs. Iceberg Classification**: Used satellite data to classify whether an image is of a ship or an iceberg.

-Quora Question Pairs: Identified question pairs with the same intent.
Parallel Fractal Generator with Multicore Programming: Developed a Java application that computes and displays the Mandelbrot set in parallel using multicore programming techniques.

Secure Bank Transactions with Blockchain and Paxos:
Implemented a mechanism for handling client transactions using Blockchain and Paxos. The bank uses Blockchain as a secure database to store all transaction information, ensuring untrusted parties reach agreement on the database state

Distributed Chat Application with Client-Server Architecture: Developed a distributed chat application with a client-server architecture. The client application handles user interface and

interactions, allowing users to communicate with each other efficiently

Web Crawler and Mini Browser: Developed a mini browser with an integrated web crawler that extracts all links from a given webpage

Android Application for Managing Professional and Client Transactions: Developed an Android application enabling professionals and clients to efficiently manage and track their transactions.

SaveCar Application for Driver and Passenger Safety: Developed SaveCar, an application aimed at enhancing driver and passenger security by monitoring and checking potential risks.

Awards & Honors

College of Computing Fellowship
Pre-doctoral fellowship at Mohammed VI Polytechnic University *October 2018 – October 2019*

Skills

Programming: Python, Bash, Slurm, HPC.
Data science stack: Numpy, Scipy, Pandas, Matplotlib, Scikit-learn, Jupyter, Pytorch, PySpark, Keras, tensorflow.
Software Design and management techniques : Merise, UML, Scrum.
Spoken Languages: Arabic (Native), French/English (Fluent).
Big Data & DBMS : Hadoop MapReduce, MySQL, Oracle, MS SQL Server, Cassandra.
Software tools: Eclipse, PyCharm, Git, Docker, Latex.
Other Interests: Debate and parallel diplomacy.